발 간 등 록 번 호
33-9750040-000444-01

비교헌법연구
2023-B-4

디지털 전환의 기본권적 문제상황과 대응체계

Constitutional Research Institute

헌법재판소
헌법재판연구원

디지털 전환의 기본권적 문제상황과 대응체계

연구책임자 : 김 태 호 책임연구관(비교헌법연구팀)

목 차

Ⅰ. 서론 / 1

1. 연구의 배경 ····· 1
   가. 지능정보기술의 혁신과 디지털 전환 ····· 1
   나. 인공지능기술과 메타버스에 따른 디지털 심화 ····· 2

2. 연구의 목적과 범위 ····· 4
   가. 디지털 전환과 디지털 헌정질서 ····· 4
   나. 디지털 전환의 기본권 보장 체계 ····· 5

3. 연구의 방법과 연구의 전개 ····· 8

Ⅱ. 디지털 전환에서 독일의 기본권적 문제상황과 대응체계 / 10

1. 연방헌법재판소에 의한 개인정보자기결정권의 발전 ····· 10
   가. 배경으로서의 정보화사회와 개인정보자기결정권의 도출 ····· 10
      1) 인격권으로서의 자기결정권 ····· 10
      2) 인구조사결정의 현대적 함의 ····· 10
   나. 디지털 전환 시대 개인정보자기결정권의 확장 ····· 12
      1) 정보 수집의 가능성 확대와 개인정보보호 ····· 13
      2) 정보 저장의 가능성 확대와 개인정보보호 ····· 16
      3) 정보의 이용 가능성 확대와 개인정보보호 ····· 19
   다. 보론: 개인정보자기결정권으로서 잊힐 권리의 인정 여부 ····· 21
      1) 디지털화에서 잊힐 권리의 맥락 ····· 22
      2) 유럽연합과 독일의 판례 발전 ····· 23
      3) 시사점 ····· 25

라. 소결 ····· 25

2. 정보기술체계의 신뢰성과 무결성 보장에 관한 기본권 ····· 27
가. 연방헌법재판소의 IT 기본권 결정 ····· 27
나. IT기본권의 법리 ····· 28
1) IT기본권의 도출근거와 내용 ····· 28
2) 정보기술시스템의 적용례 ····· 31
다. 디지털 전환의 안전장치로서 IT기본권 ····· 34
1) 개인정보자기결정권과의 차별성 ····· 34
2) 객관적 가치질서 차원의 IT기본권 ····· 36

3. 유럽연합의 디지털 전환 입법과 새로운 권리의 제도화 모색 ····· 37
가. 유럽연합의 디지털 전환 관련 주요 법률과 디지털 권리 ····· 37
1) 「유럽연합 개인정보보호법」의 디지털 권리 ····· 37
2) 「유럽연합 인공지능법」의 리스크 관리와 기본권 보장 ····· 40
나. 유럽연합 디지털 권리선언과 디지털 전환의 사회적 권리 ····· 44
1) 유럽연합 디지털 권리선언의 개요 ····· 44
2) 디지털 접근권의 강화 선언 ····· 44
3) 디지털 격차해소권의 선언 ····· 46

Ⅲ. 디지털 전환 시대의 기본권 보장 방식·체계와 국가임무 / 48

1. 디지털 전환의 변화하는 사회상 ····· 48
가. 디지털 전환을 가속화하는 디지털 기술과 사회 변화 ····· 48
1) 디지털 전환의 문제 국면들 ····· 48
2) 디지털 심화의 문제 국면들 ····· 50
나. 디지털 전환에 따른 사회 영역별 변화 ····· 51
1) 디지털 행정 ····· 51
2) 디지털 경제 ····· 51
3) 디지털 커뮤니케이션 ····· 53

2. 디지털 전환에서 디지털 기본권의 보장 ····· 54
가. 디지털 전환이 기본권에 미치는 이중적 성격 ····· 54
나. 디지털 전환의 특성을 반영한 체계적 검토의 필요성 ····· 54
1) 디지털 특성을 반영한 기본권 해석 ····· 54
2) 헌법상 권리와 법률상 권리의 구분 필요성 ····· 56
3) 디지털 전환에 대한 기본권 형성적 법률의 제·개정 ····· 56

3. 디지털 전환에 대한 기본권 대응 체계의 정비 ····· 57
가. 디지털 시대 기본권의 범주화와 헌법 개정 ····· 57
1) 광의의 디지털 기본권과 협의의 디지털 기본권 ····· 57
2) 정보기본권, 디지털 기본권, 인터넷(사이버) 기본권 ····· 58
3) 헌법 개정의 문제 ····· 58
나. 디지털화에서의 국가의 기본권 보장 체계 ····· 60
1) 기본권 존중의무 - 감시국가의 우려에 대한 경계 ····· 60
2) 기본권 보호의무와 충족의무 ····· 61
다. 사회적 형성을 통한 지속적 법제도화 필요성 ····· 62

4. 디지털화된 국가서비스의 확장과 자유의 조건 보장 ····· 64
가. 디지털 포용으로서의 디지털 권리 확장 ····· 64
1) 디지털 선택의 자유와 접근권 ····· 64
2) 디지털 포용으로서의 디지털 격차 해소권 ····· 65
나. 자유의 조건 보장으로서 국가의 개입 ····· 66

V. 요약과 결론 / 68

▌참고문헌 ····· 71

초 록

디지털 전환이란 디지털 기술의 혁신적 발전으로 사회체계와 생활 전반이 디지털화되는 총체적 변화 과정을 일컫는다. 지능정보기술의 급격한 진전으로 디지털 전환이 심화 단계에 접어들면서 인간의 가능성을 비약적으로 신장시키고 있지만, 새로운 방식의 자유 침해 가능성에 대한 우려나 자유의 조건 보장에 대한 요구 또한 커지고 있다. 헌법과 헌법재판은 이러한 구조적 변화 과정에서 발생하는 기본권적 문제 상황을 정확히 파악하고 그에 따른 기본권 보장의 요청에 응답하는 체계를 구축해야 한다.

독일 연방헌법재판소는 정보화 사회의 도래에 따라 개인정보자기결정권을 새로운 기본권으로 인정하여 다양한 디지털 기술 영역에 적극적으로 적용해 왔고, 정보기술체계의 신뢰성과 무결성 보장에 관한 기본권(IT기본권 또는 컴퓨터기본권으로도 불린다)을 창안하여 디지털 시대의 기본권 공백을 해소하고자 한 바 있다. 유럽연합에서 개인정보를 취급하는 디지털 기술, 디지털 플랫폼, 인공지능기술로 인한 리스크에 대응하여 제정한 법률들은 디지털 전환에서의 주요 규범으로 발전하고 있다. 디지털 전환에서의 규범적 수요로서 디지털 접근권, AI 알고리즘에 관한 권리, 디지털 격차해소권 등의 기본권 주장은 개별 법률 규정과 연성법적 형태의 권리 선언을 통해 형성중이다.

한국의 경우에도 디지털 전환에서의 기본권 수요를 구현하기 위해 현행헌법상 기본권을 디지털 전환의 특징을 반영하여 적용하거나, 독자적인 디지털 시대의 기본권을 도출하거나, 디지털 전환의 변화를 반영하여 헌법을 개정하는 방식 등을 순차적으로 생각해 볼 수 있다. 헌법의 방향 제시에 유의하여 디지털 시대의 자유 제한의 조건에 대해 명확히 규율하고 디지털 포용 등을 위한 구체적 법제도를 정비하는 것은 입법자의 몫이다. 디지털 전환이 감시사회를 낳는 부작용 없이 기본권적 가치를 충실히 구현하고 궁극적으로는 개인의 인격 실현에 이바지할 수 있도록 제도를 형성할 책임이 국가에 있다.

주제어: 디지털 전환, 디지털 심화, 지능정보기술, 개인정보자기결정권, IT기본권, 디지털 접근권, AI 알고리즘에 관한 권리, 디지털 격차해소권, 디지털 포용, 디지털 권리장전

Ⅰ. 서론

1. 연구의 배경

가. 지능정보기술의 혁신과 디지털 전환

인터넷을 매개로 전자화된 데이터를 생산하고 활용하는 정보통신기술(Information and Communications Technology, ICT)이 비약적인 발전을 거듭하면서 사회 체계와 소통·교류의 활동 전반이 디지털화된 형식을 통해 형성되는 비중이 커져 가고 있다. 디지털화는 아날로그적인 실물이나 공정을 디지털 신호로 전환하고, 생성한 디지털 데이터를 저장·이용하는 기술적 과정(**Digitization**)을 거쳐 디지털 기술·디지털 매체·디지털 인프라·디지털 서비스를 통해 생활양식을 변화시키는 과정(**Digitalization**)을 가리킨다. 사회·경제·문화 전반에 미친 디지털화의 영향은 생활양식 전반에 질적인 변화를 가져왔는데, 이러한 현상은 각각의 영역에서 '디지털 사회', '디지털 경제', '디지털 문화'로 별칭되고 있기도 하다. 이처럼 디지털화와 관련한 기술이 혁신적으로 발전하면서 사회 체계와 활동 전반이 디지털화되는 총체적 변화 과정을 일컬어 **디지털 전환(Digital Transformation**, DX)이라 한다.

디지털 전환은 범용성을 갖춘 디지털 혁신기술의 발전을 동력으로 삼는다. 최근의 디지털기술 발전은 속도, 범위, 영향에 있어서 사회에 근본적이고 질적인 변화를 가져왔다는 점에서 증기, 전기, 개인용 컴퓨터가 산업에 가져온 혁명적 변화에 맞먹는 **제4차**의 **산업혁명**이 일어나고 있다고 평가되기도 한다. 이 과정에서 코로나19 바이러스 판데믹이 발생하자 비대면사회를 체감한 디지털 전환의 사회적 요청은 더욱 커지게 되었다. 이제 제4차 산업혁명은 ① 보편화·고도화된 디지털 네트워크(인터넷 인프라)와 스마트폰을 비롯한 모바일 기기의 보급이라는 토대 위에서, ② 지능정보기술,[1] 즉 디지털 데이터를 분

1) '**지능정보기술**'은 인공지능이 고차원적 판단기능을 수행하여 자동화·무인화를 확산시키고, 정보통신기술을 통해 정보수집, 데이터 분석, 판단추론 등의 과정을 즉각 처리하여 실시간의 응답반응이 가능하도록 하며, 보관 활용이 곤란했던 데이터를 활용하여 의미를 추출하고, 인공지능의 스스로 학습하는 능력을 통해 그 기능을 기하급수적으로 향상시켜 나간다는 특징을 가진다고 한다. 관계부처 종합, 제4차 산

석하고 활용하며 저장할 수 있는 기술(빅데이터[2], 클라우드 컴퓨팅[3]), 사람·사물을 연결하는 기술(사물인터넷[4]), 인공지능[5] 기술등이 범용성을 갖춘 기술로 발전하여(general purpose technology), ③ 물리학·생물학 등 과학 간 경계를 허물고 다양한 산업을 '융합'하여 사회 전분야의 맞춤형 디지털화를 이끌고 있다.

나. 인공지능기술과 메타버스에 따른 디지털 심화

디지털 기술이 개별 산업에서 융합되는 현상은 스마트 공장 운영, 스마트 도시 구축, 자율주행 자동차 시범실시와 같이 실제 현실에서 구현되는 과정에 있고, 물리적 객체가 디지털화된 형태로 표현되어 가상의 시뮬레이션에 사용되는 디지털 트윈(Digital Twin)

업혁명에 대응한 『지능정보사회 중장기 종합대책』, 2016. 12. 17. 참조. 대표적으로 법에서는 지능정보기술로 인공지능기술, 데이터처리기술, 사물인터넷기술, 클라우드컴퓨팅기술, 초연결지능정보통신기반기술 등을 열거한다(「지능정보화 기본법」 제2조 4호 참조). 학계에서는 이러한 지능정보기술을 활용한 사회 변화 현상을 **지능정보사회**로 지칭해 왔는데, 이를 반영하여 「지능정보화 기본법」 제2조 제5호 및 제6호는'지능정보화'를 '정보의 생산·유통 또는 활용을 기반으로 지능정보기술이나 그 밖의 다른 기술을 적용·융합하여 사회 각 분야의 활동을 가능하게 하거나 그러한 활동을 효율화·고도화하는 것'으로 정의하고, '지능정보사회'는 '지능정보화를 통하여 산업·경제, 사회·문화, 행정 등 모든 분야에서 가치를 창출하고 발전을 이끌어가는 사회'로 정의하였다.
한편, 인터넷과 지능정보기술이 활용의 차원을 넘어 융합의 기반이 됨으로써 시간·장소·사물의 제약을 넘는 사회적 네트워크가 형성되는 점에 주목하는 관점은 디지털 전환에 따른 사회 변화를 **초연결사회**(hyper-connected society)로 표현하기도 한다(초연결이란 '정보통신 및 지능정보기술 관련 기기·서비스 등 모든 것이 언제 어디서나 연결'되는 것을 가리킨다. 「지능정보화 기본법」 제2조 제9호 참조).

2) '빅데이터'(big data)는 이전과 비교할 때 차원을 달리하는 거대한 데이터 양의 규모, 취급하는 데이터의 늘어난 다양성, 데이터를 처리하는 빠른 속도(3V=Volume, Variety, Velocity)라는 특징을 가지는 방대한 정형·비정형의 데이터로서 이로부터 가치를 추출하고 결과를 분석하는 것이 정보기술의 발달로 가능하게 되었다는 점이 중요하다. 활용 가능성이 확대된 대규모의 데이터는 다른 영역과의 융합을 통해 새로운 생활양식과 산업양식을 창출하는 '21세기의 원유'(시장조사기업 가트너)로 불린다.

3) '클라우드 컴퓨팅'(cloud computing) 기술은 개별적인 인터넷망을 통해 접속할 수 있는 서버와 디지털의 저장·관리를 위한 스토리지 및 데이터베이스 등을 인터넷망으로 연결하여 언제 어디서든 데이터에 접속할 수 있도록 한다. 법에서 '클라우드컴퓨팅기술'은 '클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술로서 가상화 기술, 분산처리 기술' 등을 가리킨다고 한다(「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조 제2호).

4) '사물인터넷'(IoT, Internet of Things)은 사물이 센서와 통신기기를 통해 연결되어 양방향으로 소통함으로써 인터넷으로 연결된 사물과 사물, 사물과 인프라, 사물과 인간을 연결하는 기술을 가리킨다.

5) '인공지능'(AI, Artificial Intelligence) 기술은 기계나 컴퓨터가 전자적 방법으로 인간의 학습·추론·지각·판단과 같은 능력을 구현하는 기술을 가리킨다(「지능정보화 기본법」 제2조 제4호 가목 참조). 특히 최근의 기술발전으로 주목받고 있는 이른바 '**생성형 인공지능**'(generative AI)은 이미지 인식, 자연어 처리(NLP=Natural Language Processing) 기술 등을 통해 인간의 지능을 모방하여 스스로 대화, 이야기, 이미지 등 새로운 콘텐츠와 아이디어를 생산해 낼 수 있는 인공지능이다.

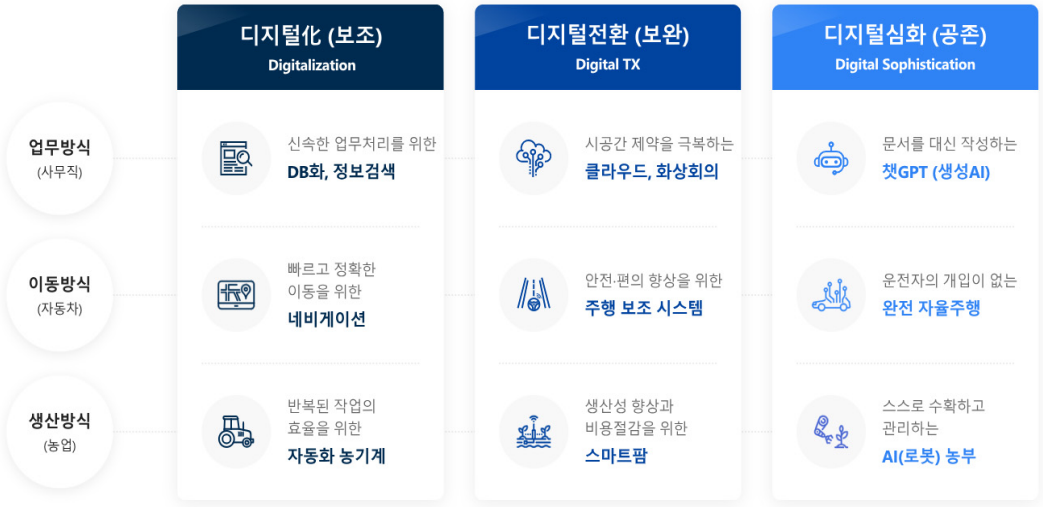
기술 등은 이미 현실에서 활용되고 있다. 우리는 이제 생성형 인공지능과 사람 간 의사소통과 유사한 행위를 흉내낸 서비스를 인터넷 공간에서 이용하기 시작하였는데, 이것이 가상현실(VR=Virtual Reality)/증강현실(AR=Augmented Reality)의 경험과 만나 멀지 않은 시기에 현실세계와 독립적으로 존재하는 가상 공간으로서의 디지털 세계(**메타버스**, Metaverse: Meta+Universe)[6]가 구축될 때 그 속에서 실존인격을 디지털화한 인간은 디지털 인간(Digital Human)으로서의 인공지능과 맺는 관계의 법적 성격을 고민하게 될 것이다. 이처럼 사회 전방위에 걸쳐 진행되고 있는 디지털 전환 현상은 바야흐로 심화단계에 접어들면서 완전히 새로운 패러다임의 사회현상을 낳으며 법제도의 대처를 요구하기 시작하고 있다.[7]

---

6) 최근 제정된 법에 따르면 '가상융합세계(메타버스)'는 '이용자의 오감을 가상공간으로 확장하거나 현실공간과 혼합하여 인간과 디지털 정보 간 상호 작용 가능하게 하는 기술을 바탕으로 다양한 사회적·경제적·문화적 활동을 할 수 있도록 구성한 가상의 공간이나 가상과 현실이 결합한 공간'으로 정의된다. 「가상융합산업 진흥법」(2024. 2. 27. 제정, 2024. 8. 28. 시행) 제2조 제1호 참조.

7) 디지털 전환의 기본원칙을 제시하기 위해 한국 행정부가 최근 제시한 '**디지털 권리장전**'(2023. 9.)에서는 디지털 전환의 고도화 국면에 주목하여 디지털 기술이 인간활동을 보완하는 것을 넘어서는 발전 국면을 일컬어 **디지털 심화**(Digital Sophistication)로 별도 분류하여 의미를 부여하고 있기도 하다(정부 인터넷사이트 '디지털 공론장', http://beingdigital.kr/front/digital_deepening_new.do 참조. 여기서 전형적인 예를 통해 설명하고자 제시된 내용이 아래 [그림]이다. 2024. 2. 29. 최종방문). 다만 디지털 심화라는 용어가 아직 세계적으로 통용되고 있는 표현은 아니므로, 이하에서는 디지털 전환을 디지털 심화를 포괄하는 개념으로 사용하면서, 고도화된 인공지능기술과 가상융합세계가 활성화된 디지털 전환 고도화 국면을 가리킬 때 필요한 경우 '디지털 심화'라는 표현을 사용하기로 한다.

[그림] 디지털화의 발전과 생활양식의 변화의 예



2. 연구의 목적과 범위

가. 디지털 전환과 디지털 헌정질서

디지털 전환이 국가·사회·개인의 생활양식에 대한 구조적이고 총체적인 패러다임 전환적 변화를 초래하는 현상이라고 한다면 그러한 현실이 가져오는 변화를 실정헌법을 중심으로 한 헌법체계가 충분히 수용할 수 있는지, 헌법체계의 그 어떤 변화가 필요한 것인지에 대해 살펴 나가는 작업이 필요할 것이다. 거시적으로 디지털 전환은 국가주권, 법치국가의 헌법적 요청과 민주주의적 헌법질서에 영향을 미치고 있다.[8] 글로벌화된 디지털 세계에서 초거대기업을 중심으로 이루어지는 디지털 경제 활동에 대해 개별 국가의 주권이 미치는 영향력은 제한되지 않을 수 없고, 이처럼 급격한 속도로 이루어지는 변화에 법적 규율이 선제적인 규율을 제시하고 법적 관계를 정비하기는 쉽지 않으며, 디지털 세계의 의사소통과 정보유통은 민주주의의 발전에 새로운 기회를 제공함과 동시에 파괴의 잠재력을 지니고 있다.

국가작용의 차원에서 디지털 전환은 입법·행정·사법활동 각 분야에서 새로운 가능성과 함께 헌법적으로 검토되어야 할 쟁점을 제기한다.[9] 모든 국가작용에서 디지털화된 절차의 구축과 의사결정 및 임무수행을 지원하는 디지털 정보의 활용 가능성이 검토되며, 궁극적으로는 최종적인 의사결정의 자동화가 어느 범위까지 허용될 수 있는지가 논의된다.

이처럼 디지털 전환이 국가·사회·개인 간 관계와 생활 양식을 근본적으로 변화시킨다면 이에 대한 헌법적 검토는 필연적인바, 디지털 전환이 가져온 현실의 헌법적 문제상황을 정확히 파악하여 최고규범으로서의 헌법적 방향성을 확립해 나가야 할 것이다.

---

8) 지능정보사회에 대한 헌법학에서의 개관으로는, 김배원, 지능정보사회와 헌법, 공법학연구 제21권 제3호, 2020, 67-80면; 김일환, 지능정보사회에서 헌법의 역할과 기능, 성균관법학 제32권 제3호, 2020, 37-92면을 참조.

9) 정보통신정책연구원, 디지털 대전환 메가트렌드 연구 총괄보고서 I, 방송통신정책연구 21-17-01, 40-48면을 참조. 코로나19 시기 인터넷을 통한 국회, 행정, 사법 작용의 가능성에 대한 논의가 디지털화의 수요를 잘 보여주었는데, 코로나19 이후에는 다시 인공지능기술의 급격한 발전이 이루어지면서 인공지능을 활용한 행정작용이나 사법작용의 가능성 및 한계에 대한 논의가 더 활발하게 되었다. 가령 김찬희, 인공지능 기반 자동화 행정행위에 관한 헌법적 고찰, 헌법재판연구원 2023; 김종현, 인공지능 법관 관련 헌법적 쟁점의 검토, 헌법재판연구원 2023.

나. 디지털 전환의 기본권 보장 체계

1) 선행연구의 접근 방식

이상과 같은 디지털 헌정질서의 정초 작업은 매우 방대한 것이어서 현실적 한계를 가진 본 보고서가 이를 담아내기에는 역부족이다. 이에 본 보고서는 디지털 헌정질서의 정초 필요성이라는 큰 틀을 염두에 두되 디지털 전환의 핵심적 헌법적 국면으로서 기본권의 보장 체계의 문제에 논의의 초점을 맞추고자 한다.

디지털 전환 현상에 대해 기본권 보장의 새로운 문제상황을 파악하고 기본권 보장의 공백을 해소하려는 선행연구가 적지 않다. 이미 인터넷이 출현하면서부터 인터넷 매체와 이를 매개로 이루어지는 활동에 대해 그 특성을 감안한 별도의 법논리를 적용하고자 하는 다양한 시도[10]들이 있었고, 최근에는 디지털화된 개인정보의 자기결정권을 중심으로 인터넷상 개인의 자유에 관한 여러 기본권이 주목의 대상이 되었다. 선행연구 중에는 익명표현의 자유, 디지털 사생활 보호권, 개인정보자기결정권, 잊힐 권리, 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권(IT기본권), 인터넷 접근권, 디지털 격차해소권, 알고리즘에 대한 설명요구권 등을 열거하면서 이를 묶어 하나의 설명적 범주[11]로서 **디지털 기본권**이라 통칭하기도 한다.

2) 연구목적에 따른 연구범위 설정 – 디지털 전환의 기본권 보장 체계

이하 본 연구에서는 최근까지의 연구성과들을 정리하는 한편, 특히 디지털 전환에 대한 헌법적 대응체계의 구축을 위해 다음의 점에 연구의 주안점을 두기로 한다.

첫째, **디지털 전환의 헌법현실**과 관련한 최근의 진전이 기본권 현실에 어떠한 근본적인 변화를 초래하고 있는지에 대한 현실적 논의를 정리하는 전제적 검토를 한다. 여기에는 특히 최근의 이른바 '디지털 심화'를 가져온 인공지능기술의 발전에 대한 언급이 추가되어야 한다. 그리고 이 때 헌법현실에 대한 판단에서는 디지털 전환이 가져올 비약적

10) 가령 로렌스 레식, 김정오 역, 코드: 사이버 공간의 법이론, 2001. 헌법재판소 역시 인터넷에 대해 '가장 참여적인 시장' '표현촉진적인 매체'라는 의미를 부여하여 인터넷 매체의 특성을 감안한 기본권 접근이 필요함을 인정한 바 있다. 헌재 2002. 6. 27. 선고 99헌마480 결정.

11) 디지털 기본권의 범주와 기능에 대해 좀 더 상세히는 이하 Ⅲ. 3.을 참조.

인 자유의 신장 가능성과 새로운 자유의 침해 가능성을 동시에 살펴야 한다. 디지털 전환이 가진 순기능과 역기능이 균형있게 고려될 필요가 있기 때문이다.

둘째, 디지털 전환의 패러다임 전환적 특성을 감안하여 그것이 초래한 기본권적 문제상황을 개별 기본권에 한정하여 검토하기보다 **기본권 체계의 관점**에서 조망하기로 한다.[12] 즉 디지털 전환을 통해 기본권적 형성과 제한의 문제가 어떤 도전을 받고 있고 그에 대한 기본권적 보장의 해법에는 어떠한 접근이 필요한 것인지를 살피는 과정에서, 특히 기본권 보장의 문제상황이 어떤 '맥락'에서 발생하고 있으며 그러한 맥락적 고려 하에서 기본권 보장의 공백을 해소하고 기본권 간의 균형을 확보하며 기본권의 본질적인 내용이 훼손되지 않도록 하는 기본권 보장의 '체계'를 구축하는 데 논의의 초점을 맞추고자 하는 것이다.

셋째, 디지털 전환에 대한 **기본권적 대응체계**로서 기본권 도출의 단계와 권리의 형성과정에 주목하기로 한다. 주지하는 바와 같이 기본권 여부를 인정하는 방식은 다양한 경로를 거칠 수 있다.[13] 명시된 개별 기본권 조항의 해석을 통해 기본권의 내용을 도출하는 방식도 있고, 복수의 기본권 조항을 결부시켜 새로운 기본권의 존재나 내용을 도출하는 방식도 있다. 기본권적 보호의 필요성이 특별히 인정되고, 권리내용이 명확하여 구체적 권리로서의 실질을 갖춘 경우[14]라면 헌법상 열거되지 않은 기본권으로서 독자적 기본권성을 인정할 수도 있다. 헌법현실에 대응하는 헌법적용 또는 헌법변천이 이루어지지 않는다면 헌법 개정이나 적극적인 입법을 할 필요가 있는지도 생각해 볼 여지가 있을 것이다.

이러한 관점에서 디지털 전환에서 문제되는 기본권 또한 현행헌법의 해석에 따른 기본권의 적용, 복수의 기본권 및 열거되지 않은 기본권으로부터 파생되는 기본권의 확장, 헌법 개정, 법률 제정을 통한 법률상 권리의 형성 또는 연성규범의 선언을 통한 규범 형성으로 각각 나누어 대응체계를 단계적으로 살펴볼 수 있을 것이다. 특히 새로운 기본권의 도출과 관련하여, 앞서 언급한 '디지털 기본권'의 범주에 포함되는 기본권들은 실정헌법의 개별 기본권으로서 명문화된 기본권이거나 해석을 통해 확립된 기본권의 내용인 경우가 대부분이지만 거슬러 올라가 보면 정보화사회가 도래하여 헌법상 기본권 목록을 확

12) 선행연구로 조소영, 지능정보사회에서의 기본권체계 및 보장내용의 변화가능성 검토, 동아법학 2022, 94호 참조.
13) 개관으로, 김하열, 헌법강의, 188-189면.
14) 헌재 2009. 5. 28. 2007헌마369 결정.

장함으로써 독자성이 인정된, 전통적 기본권에 비해 상대적으로 최근에 정립된 개인정보 자기결정권과 같은 기본권도 포함되어 있다. 이러한 기본권의 정착 과정은 새로운 디지털 기본권의 인정 가능성에 시사하는 바가 적지 않을 것이다. 이를 통해 디지털 전환이라고 하여 완전히 새로운 체계의 기본권이 필요한 것처럼 과장되는 것을 경계함과 동시에 새로운 기본권적 수요의 발생 지점을 정확히 포착할 수 있을 것이다.

3) 입법적 제도화에 대한 헌법적 평가 필요성

디지털 전환의 사회 현상에 대한 국가적 형성과 개입은 기본권의 문제 이전에 법률에 의해 형성되는 권리의 문제 또는 법률과 행정에 의한 제도적 형성의 문제로 등장하기 때문에 이러한 제도 형성의 결과를 살핀 다음 헌법적 평가를 하는 작업이 이루어질 필요가 있다. 즉 최근의 디지털 전환에서 필요하다고 제기되는 다수의 권리들은 기본권성을 획득하였다고 보기 어려워 헌법적 권리로서의 인정이 불확실하고 법률상 권리로 인정되거나 장차 인정되어야 할 권리 주장으로서의 성격을 갖는 경우가 적지 아니하다. 디지털 전환 과정에서 이러한 권리들을 법률적으로 어떻게 형성할 것인지에 대해 규범통제 등을 통한 헌법적 방향성이 제시될 필요가 있을 것이다.

우리나라의 경우에도 디지털 전환의 사회적 수요에 대해서는 행정의 대응은 물론 입법을 통한 제도화가 지속적으로 이루어지고 있다. 입법자는 개별 기술에 대한 개별법을 제정하기도 하고 개별법에서 디지털화의 수요를 반영하는 개정을 하려 하는데, 디지털 전환을 본격적인 소재로 삼아 '디지털'을 법제명에 포함시킨 법제만 보더라도 「산업 디지털 전환 촉진법」, 「디지털 기반의 원격교육 활성화 기본법」과 정부조직에 관한 대통령령인 「디지털플랫폼정부위원회의 설치 및 운영에 관한 규정」이 있다. 디지털이라는 표현을 사용하지는 않더라도 이를 주요 규율대상으로 하는 주요 일반 법률로 「지능정보화 기본법」, 「데이터 산업진흥 및 이용촉진에 관한 기본법」, 「전자정부법」 등이 있으며, 개별 지능정보기술에 대해서는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」, 「자율주행자동차 상용화 촉진 및 지원에 관한 법률」, 「가상융합산업 진흥법」 등이 있다. 디지털 기술을 접목한 융합 분야로 분류할 수 있는 법률로는 「스마트도시 조성 및 산업진흥 등에 관한 법률」, 「디지털의료제품법」 등을 열거할 수 있다. 그 밖에도 디지털화의 영향을 강하게 받은 법 개정은 매우 많은데 최근의 「개인정보보호법」이 대표적이라 할 것이다.

이러한 다종다기한 디지털 전환에 따른 법적 수요에 대해 국가의 책임은 헌법적으로 어느 정도까지 요구되는지를 보다 명확히 파악할 수 있다면 디지털 전환에 대한 시민의 권리를 어떻게 보장할 것에 대한 방법론을 좀 더 분명하게 개진할 수 있을 것이다.

3. 연구의 방법과 연구의 전개

본 연구에서는 비교법적 연구의 방법을 중심으로 연구를 진행하기로 한다. 그중에서도 독일의 기본법 해석과 연방헌법재판소의 결정례를 중심으로 독일이 정보화사회에서 시작하여 오늘의 디지털 전환에 이르기까지 헌법상 기본권에 대한 수요에 어떻게 대응해 왔는지를 살피기로 한다. 독일 기본권 해석론에 대한 비교법적 검토를 먼저 하는 것은 우리와 유사한 법체계 하에서 정보화사회의 기본권이 어떻게 전개되어 왔는지 연혁적인 과정을 살필 수 있고 기술적 발전으로 인한 기본권적 위협에 관한 주요한 논의를 통해 비교법적 시각에서 디지털 전환의 문제 맥락이 부각될 수 있으리라 판단하였기 때문이다. 독일은 연방헌법재판소가 이른바 인구조사 결정[15]으로부터 개인정보자기결정권이라는 기본권을 정립하였고, 2007년에는 정보기술체계의 신뢰성과 무결성 보장에 관한 기본권(IT기본권 또는 Computer기본권이라 한다)을 새롭게 정립한 바[16]도 있다. 또 최근에는 유럽연합 차원에서 대표적인 디지털 전환 관련법이라 할 「유럽연합 개인정보보호법」(General Data Protection Regulation, GDPR), 「디지털서비스법」(Digital Service Act, DSA)이 제정되고, 「인공지능법」(Artificial Intelligence Act, AI Act)이 제정을 앞두고 있어 해당 법의 직접 적용을 받는 유럽연합의 주요회원국인 독일에서도 다양한 논의가 진행되고 있다.

이에 이하의 논의 순서는, 우선 독일(유럽연합 포함)헌법재판에서 디지털 전환의 기본권적 수요에 어떤 체계적 대응을 전개하였는지를 살핀 다음(이하 Ⅱ.), 디지털 전환이 초래한 기본권적 문제상황과 디지털 전환에 대응하는 기본권 보장의 방식과 체계 및 국가의 책임을 검토하기로 한다(이하 Ⅲ.). 이하의 논의에서 자주 언급될 디지털 전환에서 핵심이 되는 주요 헌법조항 내지 제기되는 주요 권리를 나열하면 다음 [표]와 같다.

---

15) BVerfGE 65, 1. - 1 BvR 209/93 (1983. 12. 15. 결정)
16) BVerfGE 120, 274 − 1 BvR 370/07, 1 BvR 595/07 (2008. 2. 27. 결정).

[표] 디지털 전환에 관한 주요 헌법적 근거

기본권 목록과 근거	한국헌법	독일헌법	유럽연합 (기본권헌장·인권협약)	유럽연합 회원국	[비고]유럽 디지털 권리선언	[비고] 한국 디지털 권리장전
주요 규정	사생활의 비밀과 자유 (17조)	인격권 (2조)	사생활권, 개인정보 보호권 (헌장 7·8조) 사생활권 (협약 8조)	컴퓨터 기본권 (포르투갈 헌법 35조)	·디지털 접근권 ·정보접근권 ·디지털 안전권 ·보안권 ·디지털보호권 등 22개 조항	·디지털 표현의 자유 ·디지털 접근 ·디지털 역량 강화 ·디지털 차별 방지 ·개인정보 접근 통제 ·디지털 대체수단 요구 등 28개 조항
헌법 해석	개인정보 자기결정권	개인정보 자기결정권, IT기본권	유럽연합 법을 통한 권리 형성			
개정안	정보기본권 (2018)					

Ⅱ. 디지털 전환에서 독일의 기본권적 문제상황과 대응체계

1. 연방헌법재판소에 의한 개인정보자기결정권의 발전

가. 배경으로서의 정보화사회와 개인정보자기결정권의 도출

1) 인격권으로서의 자기결정권

사생활의 보호에 관한 헌법상 기본권 조항을 두고 있지 않은 독일에서는 판례를 통해 일반적 행동의 자유에 관한 기본권(기본법 제2조 제1항)을 인간의 존엄에 관한 기본권(기본법 제1조 제1항)과 결합하여 기본권으로서의 '일반적 인격권'을 인정해 왔다. 이 때 일반적 인격권은 자신의 정체성을 스스로 결정할 수 있는 자기결정(Selbstbestimmung)의 권리, 개인이 사적생활에서 홀로 있을 권리를 보장하는 자기유지(Selbstbewahrung)의 권리, 개인이 자신의 의사에 반하여 공개적으로 인격에 대한 공격을 받거나 염탐되는 것으로부터 방어할 자기표현(Selbstdarstellung)의 권리를 포괄한다.[17)]

정보화사회의 도래와 함께 인격권의 중요성은 나날이 커지게 되었는데 개인정보의 보호(Schutz personenbezogener Daten)에 관한 권리는 인격권의 보장체계에 포함되게 된다. 무엇보다 독일연방헌법재판소는 1983년에 이른바 인구조사결정(Volkszählungsurteil)에서 포괄적인 정보자기결정권을 일반적 인격권으로부터 도출하였다.[18)]

2) 인구조사결정의 현대적 함의

'인구조사결정'은 독일 연방의회에서 의결한 「인구조사법」에 따라 인구센서스를 실시

17) Kingreen/Poscher, Staatsrechte Ⅱ (Grundrechte), 2022, Rn. 531-538 참조.

18) BVerfGE 65, 1. - 1 BvR 209/93 (1983. 12. 15. 결정, 이하 '인구조사결정'이라 한다). 인구조사결정 이전의 발전 과정에 대해서는 김영수·김일환, 독일연방헌법법원의 인구조사판결, 헌법학과 법학의 제문제, 1996, 65면 이하; 이권일, 지능정보사회에서 개인정보자기결정권이 보호하고자 하는 헌법적 가치, 공법연구 제51권 제3호, 2023, 233면 이하를 참조. 특히 1969년의 휴가여행에 관한 분기별 의무적 통계조사에 대해 연방헌법재판소는 익명의 통계조사 자체가 위헌인 것은 아니지만, 국가가 인간의 인격을 강제적으로 기록하고 목록화하는 것이 인간의 존엄에 반할 수 있고, 국민의 인격 영역에 대한 감시가 인격의 자유로운 발현에 반할 수 있다고 언급한 바 있다(Mikrozensus 결정, BVerfGE 27, 1. 이권일, 위의 논문, 234면 참조).

하고 신고된 내용을 기록하며 이를 행정청에 전달하도록 한 것에 대한 헌법소원심판이었다. 이 사건에서 연방헌법재판소는 일반적 인격권[19]에 터잡아 개인정보에 관한 자기결정권을 도출하면서, 개인의 자유로운 인격발현은 현대의 정보처리 여건 하에서 개인정보의 무제한적인 조사, 저장, 이용과 전송에 대한 개인의 보호를 전제로 하므로, 개인정보의 이용과 유출 및 그것의 사적 이용에 대한 개인의 권리를 정보자기결정권을 통해 보장해야 한다고 하고 있다.[20]

이 판결이 오늘날에도 여전히 유효한 의미를 갖는 것은 "개인정보가 무제한적으로 조사·저장·사용 및 전달되는 오늘날의 정보처리조건"(정보처리시스템이 발달하기 시작한 1983년 당시의 표현이다)이라고 현상을 기술하면서 개인정보자기결정권에 대한 특별한 보호의 필요성을 역설하고 있기 때문이다.[21]

> "(개인정보를 신고하고 이것이 자동처리될 수 있는 것에 대해 개인정보가) "오늘날 자동정보처리의 도움으로 기술적 차원에서 무제한적으로 저장될 수 있고 언제든지 멀리서도 순식간에 인출될 수 있기 때문에 (개인정보자기결정의) 권리는 위태로운 상황이다. 나아가 이러한 신고사항은 – 특히 통합정보체계 구축의 경우에 – 다른 정보수집과 함께 결합하여 당사자가 정보의 사실 여부와 이용을 충분히 통제할 수 없는 상태에서 부분적으로 또는 광범위한 형태로 전체 인격상이 조합될 수 있다. 이에 따라 개인이 공적 참여를 할 때 지금까지 알려지지 않은 방식으로서 자신의 행동에 영향을 받을 수 있는 정보 열람과 개입에 의해 심리적 압박을 받을 가능성이 확대되었다."[22]

> "개인의 자기결정은 – 현대의 정보처리기술의 조건 하에서도 – 행동하거나 행동하지 않을 것인지, 결정에 따라 실제 행동을 할 가능성을 포함하여, 개인에게 결정할 자유가 주어져 있다는 것이 전제가 된다. (…) 개인의 자기결정은 자신에 관해 누가 무엇을 언제 그리고 어떤 기회에 알고 있는지를 국민이 더 이상 알 수 없는 사회질서 그리고 이를 가능하게 하는 법질서는 정보의 자기결정권과 양립할 수 없다. 남들과 다른 행동양식이 항상 기록되고 정보로서 계속 저장되며 이용되거나 전송되는지 여부에 대해 알지 못하는 사람은 괜히 그러한 행동을 하여 주목의 대상이 되려고 하지 않을 것이다. 가령 집회나 시민운동에 참여하는 것이 공적으로 기록된다는 것과 이에 의해 자신에게 위험이 생길 수 있다는 것을 고려하는 사람은 아마도 그에 대한 자신의 기본권(기본법 제8조, 제9조) 행사를 포기하려 할 것이다. 이는 개인의 개별적 인격발현가능성을 침해할 뿐만 아니라 공공복리도 역시 침

19) 독일의 논의에 대해서는, 김일환, 독일 기본법상 일반적 인격권의 성립과 발전, 법과 정책 제6호, 2000;
20) BVerfGE 65, 1(인구조사결정), 45.
21) BVerfGE 65, 1(인구조사결정), 41-42.
22) BVerfGE 65, 1(인구조사결정), 41-42.

해한다. 왜냐하면 자기결정은 국민의 행동력과 참여력에 근거를 둔 자유민주적 공동체의 기초적인 기능 조건이기 때문이다."[23]

"그 자체만을 놓고 볼 때 사소한 정보도 정보기술에 의한 처리 및 연결에 의해 새롭게 정보로서의 가치를 얻을 수 있다. 그러한 점에서 자동정보처리 여건 하에서 '사소한'(belanglos) 정보는 더 이상 없게 된다."[24]

이처럼 이 결정은 오늘날에서도 문제되는 정보의 결합, 즉 인구 조사를 통한 정보 수집이 기록의 형태로 수집되고 그러한 정보가 상급관청으로 전달되는 것이 헌법에 위반된다고 한 점에서 정보체계에 대한 기본권 보장의 핵심적 쟁점을 다루고 있다.

또한 독일의 경우 일반적 인격권의 발전은 당초 사생활의 보호로서의 측면에 중점을 두었다가 개인이 외부에 드러나는 자신의 인격상을 결정할 수 있는 권리 또는 개인이 자신의 의사에 반하거나 자신이 모르는 채 인격상이 형성되는 것을 통제할 수 있도록 하는 적극적 권리를 보장하려 한다. 이는 인격권의 내용으로서 '자기결정'을 넘어 '자기표현'의 권리까지 개인정보자기결정권을 통해 보장하려 한 것이다. 즉 적극적인 의미로서 개인정보자기결정권은 "외부 혹은 제3자에 드러낼 나의 인격상에 대해 스스로 결정할 수 있는 권리(자기표현권) 혹은 나의 인격상이 나의 의사에 반하여 혹은 나도 모르게 타자에 의해 형성되지 않도록 통제할 수 있는 권리"[25]로 확장된 것으로 평가된다. 이를 통해 개인정보자기결정권은 디지털화에 따라 정보가 쉽게 저장·유포되는 상황에서 개인이 자신의 정보를 통제할 수 있는 기본권으로서의 독자적 위상을 강화하게 된 것으로 평가된다.

나. 디지털 전환 시대 개인정보자기결정권의 확장

인구조사결정 이후 독일에서 「인구조사법」이 개정된 것은 물론이고 정보보호법제가 개정되어 개인정보보호에 대한 법률 차원의 규율이 정비되었다. 이하에서는 이러한 과정에서 개인정보의 수집·저장·이용 각 단계에서 개인정보보호권이 문제된 대표적인 결정의 예들을 통해 독일에서 개인정보보호권의 쟁점들을 일별해 보기로 한다.

---

23) BVerfGE 65, 1(인구조사결정), 42-43.
24) BVerfGE 65, 1(인구조사결정), 45.
25) 이권일, 위의 논문(2023), 241면.

1) 정보 수집의 가능성 확대와 개인정보보호

정보의 중요성이 커지는 만큼 안전 등 공익을 목적으로 한 행정의 정보수집 활동이 활발해지면서 경찰을 중심으로 한 행정의 정보활동이 점점 더 문제된다. 이는 공공장소에서 감시카메라나 CCTV를 통한 정보수집[26], 생체정보 등의 수집에 대한 법적 규율에서 문제되어 왔다.

이에 관한 대표적인 사례으로 독일에서 이동하는 차량의 번호판 정보를 감시카메라를 설치하여 무차별적으로 수집하는 것에 대한 헌법소원이 있었다. 독일의 주 법률은 감시카메라를 통해 공공장소에서 차량번호판을 수집할 수 있도록 허용하는 조항을 두고 있었던바, 수집한 정보를 경찰 수배명단에 있는 특정데이터와 대조·확인하여 도난 차량이나 허가되지 않은 차량을 포착하는 목적으로 활용하고 있었다.

(가) 감시카메라에 의한 자동화된 차량번호판 정보 수집 결정 I

헤센주와 슐레스비히-홀스타인 공공 장소의 정보수집에 관한 주 경찰법에서 차량번호판을 자동화하여 수집할 수 있도록 한 규정에 대한 헌법소원 사건에서 연방헌법재판소는 촬영된 번호판과 수배대상의 비교가 즉각적으로 이루어지지 않거나 이후 곧바로 삭제되지 않는다면 정보의 자기결정권을 침해하는 것이라고 판단하였다.[27]

> "개인정보자기결정권은 특히 현대의 정보처리 여건 하에서 정보관련조치로 인해 인격을 침해하거나 위험에 처하게 하는 것을 취급한다. 이 권리는 행동의 자유와 사생활의 기본권적 보호를 보장하고 확장하는데, 인격이 위험에 처하는 단계에서 이미 보호가 시작된다."[28]

> "전자적 정보처리조치로 인한 침해의 잠재성이 갖는 특수성은 종래의 방식으로 전혀 대처할 수 없는 처리될 수 있는 정보의 양에 있다. 그러한 기술적 가능성과 동반하여 증가한 이러한 위험상황이 기본권 보호의 문제에 해당한다.
>
> 더 큰 데이터베이스를 구축하는 것이 궁극적으로 해당범위를 더 줄이기 위한 수단일지라도 정보를 행정청으로 하여금 이용가능하게 하고 검색을 통해 추후 비교할 수 있게 한다면 정보처리가 이미 기본권을 제한하는 것이다. 감독과 이용의 목적에 따라 정해지는 관련성을 전체적으로 고려할 때 기본권 제한을 가져올 만한 질적인 성격의 것이라고 인정할 수

26) 독일연방헌법재판소는 CCTV 녹화의 경우 해당 공공장소에 방문하는 잠재적 방문자의 개인정보자기결정권에 대한 제한하여 명확하고 비례원칙에 부합하는 법적 근거가 필요하다고 하고 있다. BVerfGE NVwZ 2007, 688 (690).

27) BVerfGE 120, 378 - 1 BvR 2074/05 (2008. 3. 11. 결정, KfZ-Kennzeichen I).

28) BVerfGE 120, 378, 397.

있는 방식으로 행정청이 해당 정보를 이용하는 이익을 취했는가가 결정적이다.

개인정보자기결정권의 보호범위는 이미 그 성격상 민감하고 기본권적으로 보호되어야 하는 정보에 한정되지 않는다. 그 자체로 정보의 내용이 적은 개인정보처리도 그 목적과 정보의 처리 및 결합가능성에 따라 관련자의 사생활과 행동의 자유에 중대한 영향을 미칠 수 있다. 그 점에서 전자적 정보처리의 여건 하에서 사용의 맥락과 관계없이 그 자체 사소한 개인정보란 존재하지 않는다."[29]

"관련 정보가 공개적으로 이용 가능하더라도 기본권의 보호는 사라지지 않는다. 개인이 정보를 공개하더라도 자신과 관련된 개인정보가 자동화된 정보 수집 과정에서 저장되고 재사용될 가능성을 위해 수집되지 않을 이익을 개인정보자기결정권은 보호한다."[30]

"저장과 이용을 위해 이루어진 번호판 수집은 이미 관련자의 개인정보자기결정권을 제한하는데, 수집을 통해 추가적 조치를 위한 기반으로서의 개인정보를 행정에게 제공하는 것이기 때문이다. 자동번호판 인식과 관련한 제한은 그것이 개별 사안의 확인을 기술적으로 용이하게 하는 것일 뿐만 아니라 최단기에 다수의 연속된 번호판을 인식할 수 있도록 한다는 점이 특징적이다. 여기에 추가적 정보, 가령 자동차의 위치나 목적지에 관한 정보가 저장된다면 개인정보자기결정권의 더 강한 제한이 이루어지는 것이 된다(…)."[31]

이상의 설시에 비추어 연방헌법재판소는 감시카메라에 의한 차량번호판의 수집이 초래한 기본권 제한은 비례원칙에 부합하는 일정한 조건 하에서만 정당화될 수 있다고 보았다. 즉 해당 번호판수집이 수권근거조항의 목적 자체(이 사건의 경우 수배자 추적)를 위하여 활용되어야 하고, 이후에 관련 개인정보가 저장되어 남거나 다른 경찰적 조치의 기초로 활용되어서는 안 된다. 그리고 차량번호판 통제와 같은 감시의 경우 입법자는 제한의 한계, 사실적 근거, 보호되어야 할 법익의 비중을 규정하여 제한되는 기본권과 그 정당화 간의 균형을 확보해야 한다고 하였다.[32]

(나) 감시카메라에 의한 자동화된 차량번호판 정보 수집 결정 II

이후 연방헌법재판소는 자동 차량번호 감시를 허용한 바이에른주 경찰법에 대한 헌법소원에서 2008년의 차량번호판 정보 수집 결정의 취지를 이어서 기본권 침해 여부에 대한 엄격한 심사를 한다.[33] 바이에른주 경찰법에 따르면 지나가는 차량번호를 판독한 결

29) BVerfGE 120, 378, 398.
30) BVerfGE 120, 378, 399.
31) BVerfGE 120, 378, 400-401.
32) BVerfGE 120, 378, 429.
33) BVerfGE 150, 244 - 1 BvR 142/15 (2018. 12. 18. 결정, KfZ-Kennzeichen II).

과를 데이터 세트로 변환하여 지명수배 정보의 데이터베이스와 비교한 후 삭제하도록 되어 있었다. 이에 대해 연방헌법재판소는 일정한 경우 정보가 추후 즉시 삭제된다고 하더라도 차량번호 감시를 받는 모든 사람들의 개인정보자기결정권 제한은 비례원칙 위반에 해당할 수 있다고 판단하였다. 즉 차량번호를 통한 감시는 충분히 구체적이고 객관적인 이유가 있고, 상당히 중대한 법익 또는 비교적 중요한 공익의 보호를 위한 것이며, 개인정보보호권의 차원에서 수인가능하여 헌법적으로 받아들일 만한 것이어야 하고, 투명성, 권리구제가능성, 감독, 데이터 이용 및 삭제 규정의 규율이 포괄적으로 구비될 때에만 정당화될 수 있다고 판단하였다.[34)]

> "사람 또는 물건을 추적하기 위한 자동적 차량번호판 통제는 전체적으로 중대한 제한이다. (…) 이 때 통제는 차량번호에만 관련되고, 직접적으로 개인의 특성이나 속성과 관련성을 갖지 않으며, 인적관련성은 간접적으로만 만들어진다. 여기서 또한 중요한 것은, 장소, 날짜, 시간 및 이동 방향만 수집되고 사람이나 차량은 수집되지 않는다는 것이다. 그 밖에도 이 통제가 압도적인 수의 해당자에 대해 전혀 직접적인 부정적 결과가 결부되지 않고 어떤 흔적도 남지지 않아야 한다는 점도 특별히 고려되어야 한다. 데이터 비교가 단 몇 초만에 이루어지고 수집된 정보가 관련이 없는 것이면 그 누구도 모르게 즉각 완전히 삭제된다는 사실은 제한의 중대성을 상당히 완화한다.
>
> 이러한 통제가 그 원칙에 따라 객관적으로 위험상황에 처한 사람에 한정되지 않고, 처음부터 위험 유발과 무관한 불특정한 다수의 사람에게까지 미친다는 점이 제한의 중대성이 강화한다. 이러한 통제는 실제 누구에게 해당될 수 있다. 이러한 정보수집은 제한의 중대성을 강화한다. 나아가 이러한 조치가 은밀하게 이루어진다는 사실은 더욱 부담으로 작용한다. 추적을 목적으로 수많은 사람을 상대로 한 공공장소에서 이뤄지는 연속적 감시와 같은 광범위한 수사는 감시를 받는 느낌을 유발할 수 있다. 번호판 통제를 통해 포착되는 사람들이 문제되는 사례가 아닌 경우에는 이를 알아차리지 못한다는 것이 제한의 비중을 없애지 못한다. 왜냐하면 이를 통해 조치에 따른 성가심은 없어지지만 그것의 통제적 특성과 그에 따른 사회 전반의 자유로움과도 관련한 개인적 자유의 제한은 없어지지 않는다."[35)]

이러한 법익보호의 중요성과 비례원칙의 엄격한 적용을 통해 연방헌법재판소는 정보수집을 위한 수단으로서 감시카메라를 통한 정보수집을 정한 법률규정의 무효를 선언하면서, 감시조치의 발동근거가 되는 보호법익을 상당히 중대한 법익 또는 비교적 중요한 공익의 보호를 위한 것으로 한정하고, 필요한 장소적 범위를 제한하며, 차량번호 감시 조

34) BVerfGE 150, 244, 280-281.
35) BVerfGE 150, 244, 282-283.

치의 실시를 위한 결정의 근거를 문서화하도록 요구하였다.

2) 정보 저장의 가능성 확대와 개인정보보호

정보통신기술의 발달로 일상활동의 기록이 자동적으로 수집되더라도 수집된 정보의 저장 및 보관을 규율하는 것이 개인정보보호에서 매우 중요하다. 이와 관련하여 스마트폰의 보급 등 통신기기 사용으로 발생하는 개인정보의 보호가 문제되는 대표적인 사례가 통신데이터의 저장문제이다. 무엇보다 통신데이터는 정보주체의 습관, 체류장소, 인간관계 등을 저장하는 결과가 발생하므로 해당 정보가, 아무런 제한없이, 향후 사용될 가능성을 전제로 하여 임의 저장·보관되는 것은 사생활에 대한 위축 효과를 발생시킨다.[36] 통신데이터의 경우 통신의 비밀에 관한 기본권(기본법 제10조 제1항) 제한의 보호범위에 속하는데 데이터의 '저장'이 초래하는 기본권 침해 판단의 맥락은 개인정보자기결정권 침해 판단에서와 맥락을 같이 한다. 이에 연방헌법재판소의 결정과 함께 유럽연합의 유럽사법재판소[37]의 결정을 비교하여 살펴볼 필요가 있다.

가) 통신데이터 저장 의무화에 대한 연방헌법재판소의 결정

독일 연방헌법재판소는 2007년 통신감시에 관한 법 개정을 통해 연방통신법 및 형사소송법 규정이 개정된 후 제기된 헌법소원에서 통신데이터 저장에 관한 세부 규율이 위헌이라는 판단을 하였다.[38] 즉 통신데이터에는 유무선 전화기록, SMS, MMS, 전자우편 내지 온라인접속기록이 모두 포함되는데, 통신서비스사업자에게 이 데이터를 6개월 동안 보관할 의무를 부여하고 이후 1개월 이내에 삭제하도록 하는 것이 법 개정의 주요 내용이었다. 법 개정은 기실 유럽연합의 통신데이터저장지침(2006/24/EC)을 회원국인 독일이 전환한 내용이었으나, 구체적인 규율은 독일 입법자에 의해 이루어진 것이다. 여기서 독일 통신법은 저장된 통신데이터가 이용될 수 있는 목적에 대해 규율하고 있긴 하였지만 이는 일반적인 내용으로서 후속입법으로 연결고리가 되는 규범(Scharniernorm)이지 수권규범이 아니었다.

이 사건에서 연방헌법재판소는 데이터 안전과 관련하여 안전기준이 명확하고 구속력

---

36) 정애령, 독일 통신데이터저장제도의 비판적 고찰, 공법연구 제45집 제3호, 2017. 2. 127면.

37) Gerichtshof der Europäischen Union/Court of Justice of the European Union

38) BVerfGE 125, 260 - 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08 (2010. 3. 2. 결정). 이 결정에서는 재판관 2인의 반대의견이 있었다.

있는 방식으로 법에서 규율되어야 하고, 전문가들의 논의와 새로운 과학기술적 인식에 따른 업데이트를 거쳐 기준이 정해져야 하며, 단순히 일반적인 경제적 관점의 형량을 해서 결정하도록 맡겨서는 안 된다고 보았다. 그리고 또한 데이터 안전이 충분히 확보되어야 하며, 데이터 이용은 그것이 법익보호를 위해 상당한 중요성을 가지는 임무를 위한 경우에만 비례원칙에 부합할 수 있다고 보았다. 가령 형사소송의 경우 중범죄의 구성요건을 충족하였다는 의심이 있는 경우로 한정하여야 하고, 위험방지나 국가안보 목적의 경우에도 개인의 생명·신체·자유에 대한 구체적인 위험이나 연방과 주의 존립과 안전에 대한 위험이 존재한다는 사실상의 판단근거가 있어야만 한다고 보았다.[39]

이에 따라 연방헌법재판소는 통신데이터를 저장하는 것 자체는 위험방지 목적 등을 위해 정당화될 수 있으나, 데이터 저장에 관한 심판대상 법률의 규율은 데이터 안전을 충분히 보장하고 있지 못하고, 기본권 제한의 중대성을 충분히 고려하지 않은채 데이터의 이용 목적에 대해 제대로 범위를 제한하고 있지 않으며, 데이터제공에 대한 규율이 투명하지 않은 등 기본권 제한이 비례원칙에 위배되어 무효라고 선언하였다.

나) 통신데이터 저장 의무화에 대한 유럽사법재판소의 결정

유럽사법재판소는 위에서 위헌결정이 이루어진 독일 입법의 출발이 되었던 유럽연합 통신데이터저장지침(2006/24/EC)에 대해 유럽연합 기본권 헌장에 따른 사생활권과 개인정보보호권의 제한에 대해 명확하고 정교한 규율을 하지 않았고, 데이터 남용의 리스크와 불법적 데이터 접근 가능성을 방지하기 위해 충분한 안전장치를 두지 않았다는 이유로 무효를 선언하였다.[40]

그리고 이후에도 당시 유럽연합 회원국이었던 영국과 스웨덴의 국내 법률이 안전 및 테러 대응을 위해 통신데이터를 저장할 수 있도록 한 규율에 대해 그것이 유럽법에 부합하는지 선결적 판단을 제청한 사건에서 해당 국가의 법률이 유럽법 차원에서 허용되지 않는다고 보았다.[41] 이 때 유럽사법재판소는 심사기준으로서 유럽연합기본권헌장의 기본권 규율 외에도 유럽연합데이터보호지침[42]에 위배된다고 판단하였다. 사생활권과 개인정

39) BVerfGE 125, 260, 260 (Leitsätze).

40) EuGH, 2014. 4. 8. C-293/12 (Digital Rights Ireland Ltd.), C-594/12 (Kärntner Landesregierung).

41) EuGH, 2016. 12. 21. C-203/15, C-698/15 = NVwZ 2017, 1025. 사건 개요 등 자세히는 이상학, 위험방지를 위한 정보활동의 가능성과 한계–통신데이터저장제도에 관한 EU사법재판소의 판결을 중심으로, 헌법학연구 제25권 제2호, 2019. 6. 91면 이하; 같은이, 독일 통신데이터저장법률에 관한 소고 – EU 사법재판소의 판결을 기준으로, 홍익법학 제21권 제1호, 2020. 2. 432면 이하를 참조.

42) 이는 유럽연합 개인정보보호법(GDPR)의 모태가 된 유럽연합 데이터보호지침을 가리킨다. Richtlinie

보호권의 제한은 필요한 범위에 한정되어야 하는데 모든 통신데이터를 무차별적으로 저장하도록 한 회원국의 규정은 비례원칙에 위배된다고 판단하였다.[43]

다) 독일의 후속 입법과 유럽사법재판소의 판단

이상의 결정으로 유럽연합 회원국인 독일에게 통신데이터를 저장하도록 규율할 의무도, 이를 광범위하게 정할 수 있는 여지도 없어졌다고 할 수 있었는데, 그럼에도 불구하고 독일은 다시 2015. 10. 16. 통신법과 형사소송법을 개정하기 위해 "통신데이터의 저장의무 및 최장저장기간의 도입을 위한 법률(이하 통신데이터저장법률)"을 제정하였다.[44] 이에 따라 통신법과 형사소송법에서는 데이터 수집과 이용에 대해 엄격히 특정 목적에 한정된다는 원칙을 두고, 형사소송법에는 '통신데이터의 수집'에 대한 절차법적 규율과 보관된 데이터의 요청에 대비한 데이터 종류별 저장의무 기간을 두고, 통신법에 데이터 저장의무와 관련한 조항(제113a조, 제113b조), 데이터 이용에 관한 조항(제113c조), 데이터안전확보와 관련한 4개의 조항(제113d조-제113g조)이 추가되었다. 이는 앞서 본 연방헌법재판소의 위헌결정을 반영한 것이기도 하였다. 그럼에도 이 법이 일정한 제한 하에 통신데이터의 저장 규정을 두었던 것은 연방헌법재판소가 데이터 저장에 대해 기본권의 중대한 제한이기는 하지만 그러한 활동이 전면적으로 금지되는 성질의 것은 아니라고 판단하였기 때문이다.

그런데 관련하여 인터넷 사업자 Spacenet와 Deutsche Telecom이 2015년 제기한 사업자의 저장의무에 대한 독일의 행정소송 과정에서 행정법원은 다시 유럽사법재판소에 유럽법의 위반 여부에 대해 선결적 판단을 제청하였다. 데이터 저장이 전면적으로 금지되는지 아니면 제한적 요건 하에서는 저장이 허용되는지에 대한 판단이 필요했던 것이다. 이에 대해 유럽사법재판소는 통신데이터를 10일에서 4주 동안 통신 및 위치데이터를 저장하도록 한 개정 독일 통신법 조항이 여전히 유럽법에 위반된다는 선언을 하면서 회원국에서 저장의무를 부과할 수 있는 기준을 적극적으로 제시하였다.[45]

2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), ABl. 2002 L 201, 37.

43) 이와 관련하여 기본권 보장에 대한 유럽사법재판소의 역할에 대해서는, Kühling, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, 681을 참조.

44) 개정법률의 세부적 내용은 정애령, 위의 논문(2017), 135면 이하를 참조.

45) EuGH 2022. 9. 20. SpaceNet AG u.a., C-793/19, C-794/19, EU:C:2022:702. 자세히는 박희영, 독일 통신사실확인자료 보관조항의 EU 법 위반과 형사정책적 시사점, 형사정책연구 제34권 제1호, 2023. 유럽사법재판소의 결정 이후 연방헌법재판소는 계속중이던 헌법소원에 대해 심사불회부 결정을 하였다

이러한 유럽사법재판소의 태도는 영국 등 여타 회원국에서의 규정에 대해 제기된 선결적 판단 제청 사건[46]에서 통신데이터의 저장은 예외적으로 인터넷에서의 중대범죄나 현재 또는 임박한 국가안보 위협에 대응하는 경우에 한하여 엄격한 요건 하에 활용될 수 있다고 한 것의 연장선상에 있다.

3) 정보의 이용 가능성 확대와 개인정보보호

가) 국가안보와 관련한 법령에서 데이터이용에 관한 결정

국가안보 등 상대적으로 중대한 법익을 위한 기본권 제한과 관련한 사안들에서도 독일 연방헌법재판소는 최근까지 계속하여 그 이용 가능성을 제한하고 있다.

연방헌법재판소는 통신사업자가 이용자와 계약을 체결하면서 제공받는 이름, 주소, 생년월일 등 기본적인 가입자정보의 제공에 관한 규정이 가입자정보의 제공을 통해 가입자의 통신정보나 특정시점에 할당된 IP주소를 알 수 있게 하여 가입자의 개인정보자기결정권 및 통신비밀에 관한 기본권을 침해한다고 하였다.[47] 또 연방정보원이 통신네트워크에서 일정한 검색어를 통해 외교안보와 관련된 정보를 수집할 수 있도록 한 이른바 '전략적 해외통신감시'에 관한 조항[48]이나 대테러전산자료로 저장된 데이터베이스를 데이터마이닝을 통해 확장 사용할 수 있도록 한 테러 대응을 위한 전산자료법 조항에 대해 그 허용요건이 불충분함을 들어 위헌 결정을 한 바 있다.[49] 이러한 결정은 정보기관 또는 정보기관과 경찰기관 간의 정보 교환을 통해 발생할 수 있는 기본권 침해의 가능성을 엄격히 제한하기 위한 요건들을 두고자 하는 노력으로 이해된다. 대표적으로 바이에른 주의 헌법보호법이 데이터 수집, 처리 및 공유 권한을 광범위하게 인정한 것에 대해 개인정보자기결정권, 통신비밀에 관한 기본권 등을 침해한다고 판단한 바 있다.[50]

나) 예측적 경찰활동을 위한 데이터베이스 이용에 대한 결정

데이터의 활용도가 증가하면서 공권력 행사기관이 이를 무분별하게 활용하려 할 경우

(BVerfGE 2023. 2. 14/15, - 1 BvR 141/16, 1 BvR 2683/16, 1 BvR 2845/16).

46) EuGH 2020. 10. 6. - C-623/17, ECLI:EU:C:2020:790.

47) BVerfGE 2020. 5. 27 - 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II).

48) BVerfGE 2020. 5. 19 − 1 BvR 2835/17.

49) BVerfGE 2020. 11. 10 − 1 BvR 3214/15. 관련 내용은, 이지효, 대테러전산자료법의 데이터마이닝 허용규정에 대한 위헌 결정, 세계헌법재판 조사연구보고서 2021년 제4호, 2021. 7. 참조.

50) BVerfGE 2022. 4. 26 - 1 BvR 1619/17. 관련 내용은, 김태호, 바이에른 주 헌법보호법에 따른 정보기관의 정보 수집·공유 권한, 세계헌법재판 조사연구보고서 2022년 제5호, 2022. 7. 참조.

다양한 기본권 침해의 문제상황을 초래할 수 있음은 주지의 사실이다. 방대한 데이터가 수집되고 이를 다시 인공지능 등을 이용한 분석기법을 동원하여 활용하게 된다면 개인의 인격에 미치는 파급효과는 차원을 달리하는 것이 될 수 있다. 이와 관련하여 최근 독일에서는 범죄 예방을 위하여 경찰이 자동화 시스템을 통한 데이터 처리 권한을 가질 수 있도록 일부 주에서 경찰법 규정을 개정하였고, 이에 대해 연방헌법재판소가 위헌 결정을 한 사건이 있었다.[51] 이 결정은 경찰이 수집한 정보를 데이터 처리 시스템을 통해 재차 분석하여 판단할 경우 발생할 수 있는 기본권 침해의 문제를 살폈다는 점에서 중요한 의미를 가진다.

연방헌법재판소는 데이터의 이용이 정보자기결정권을 제한한다고 하였다. 즉 데이터 분석·평가를 위한 자동화된 애플리케이션을 사용하여 저장된 데이터를 처리할 때, 처리 과정에서 종전에는 결합되어 있지 않던 데이터를 추가적으로 이용하는 경우뿐만 아니라 자동화된 데이터 분석·평가를 통해 특히 기본권과 관련한 새로운 정보를 획득할 수 있게 되므로 정보적 자기결정이 제한될 수 있다고 보았다. 그런 다음 경찰이 안전 목적으로 데이터를 활용하는 데 대해 개인정보자기결정권의 침해 여부를 다음과 같이 엄격한 비례원칙을 적용하여 판단하였다.[52]

연방헌법재판소는 자동화된 데이터 분석·평가 조치로 인해 초래되는 기본권 제한에 대해서 별도의 평가가 필요하다고 보았는데, “한번 수집되고 저장된 데이터를 자동화된 데이터 분석·평가 시스템을 통해 추가 처리하는 것은 당초의 수집으로 인한 기본권 제한의 정도를 넘어서 별도의 부담을 주는 효과를 낳는 것”이기 때문이다. 따라서 기존의 정보를 수집하고 저장하는 것을 넘어 이를 독자적인 알고리즘에 넣어 자동화된 데이터 분석·평가 조치를 하는 데 대해서는 다음과 같이 엄격한 비례원칙에 따른 심사가 필요하다고 보았다.[53]

> 자동화된 분석·평가는, 그것이 많은 양의 복잡한 정보 처리를 가능하게 한다는 점에서 더 나아간 것으로 볼 수 있다. 분석 방법에 따라서는 기존 데이터를 링크(연결)한 평가를 통해 새로운 개인 관련 데이터가 획득될 수 있는데, 그 새로운 정보는 이러한 방법이 아니고서는 접근이 어려운 정보이다. 이러한 조치는 데이터가 담고 있는 정보를 이전보다 더

51) 자세히는 김태호, 범죄 예방을 위하여 경찰에 부여된, 자동화 시스템을 통한 데이터 처리 권한의 위헌성, 세계헌법재판 조사연구보고서 2023년 제3호, 2023. 5. 참조.
52) 연방헌법재판소 2023. 2. 16. 결정, 1 BvR 1547/19, 1 BvR 2634/20.
53) 김태호, 위의 조사연구보고서 2023년 제3호, 7-11면에서 발췌.

강도 높게 추출하는 것이다. 이 과정은 데이터에 존재하는, 링크 조치가 아니라면 숨겨져 있을 개인에 대한 인식을 생성하게 할 뿐만 아니라, 투입되는 내용에 따라 프로파일링 행위에 근접하는 것이 될 수 있다. 왜냐하면 해당 소프트웨어가 문제된 사람의 주변으로부터의 관계와 관련성에 대한 데이터 및 알고리즘 가정까지 끌어들임으로써 한 사람에 대한 완성된 상을 창출하는 새로운 가능성이 열릴 수 있기 때문이다. 따라서 목적 구속의 원칙을 두는 것만으로는 그 기본권 제한의 중대성을 충분히 고려하지 못하게 될 수 있다.

복잡한 형태의 데이터 크로스체크 기법을 사용하는 경우 그로 인한 기본권 제한이 특히 문제될 수 있다. 전체적으로 볼 때 자동화된 데이터 분석·평가 방법을 통해 획득되는 개인에 대한 인식이 광범위하고 깊을수록, 오류 발생과 차별 가능성이 높을수록, 소프트웨어에 의존한 링크를 사후 검증하는 것이 어려울수록, 자동화된 데이터 분석·평가 방법의 제한 강도는 크다고 할 것이다.

자동화된 데이터 이용이 정보 자기결정에 대한 중대한 제한을 야기할 수 있다면, 이러한 제한은 통상 강도 높은 제한에 속하는 비밀 감시조치에서 적용되는 엄격한 허용요건을 충족시킬 수 있을 때 정당화된다. 이 경우 조치는 개인의 생명, 신체, 자유와 같이 특히 중요한 법익의 보호를 위한 경우에만 허용된다. 여기서 헌법적으로 필요한 제한조치의 허용기준으로서 충분히 구체화된 위험(hinreichend konkretisierte Gefahr)이 요구된다.

특별하게 중요한 법익 보호를 위한 조치의 허용기준으로서 구체화된 위험 기준을 두지 않는 것을 헌법적으로 용인하려면, 자동화된 분석·평가의 허용 여부를 규범적으로 명확히 정하고 허용되는 조치에 따른 기본권 제한의 강도가 상당히 약화될 정도로 관련 사항을 좁게 한정하여야 한다.

경찰은 한 번의 클릭으로 개인, 그룹 및 모임에 대한 포괄적인 프로파일을 만들 수 있다. 법적으로 결백한 많은 사람들의 데이터가 그 어떤 맥락에서 수집된 다음 그 데이터에 대한 자동화된 평가가 경찰로 하여금 그들을 용의자로서 잘못 인식하게 하는 경우에 경찰은 이들이 추가적인 경찰 조치에 연루되게 할 수도 있다. 따라서 이러한 조치를 위해서는 특히 중요한 법익에 대한 구체화된 위험이 요구된다.

다. 보론: 개인정보자기결정권으로서 잊힐 권리의 인정 여부

이른바 '잊힐 권리'의 기본권성 인정과 도출 근거에 대해서는 다양한 견해 대립이 있다.[54] 이하에서는 디지털 전환 과정에서 등장하는 새로운 권리 수요와 그것의 기본권성

54) 관련 논의로, 가령 이권일, 디지털 데이터와 잊혀질 권리, 저스티스 194-2호, 2023, 179-189면 참조.

인정 조건이라는 관점에서 유럽연합과 독일에서의 '잊힐 권리' 논의를 좀 더 살펴보기로 한다.

1) 디지털화에서 잊힐 권리의 맥락

최초 유럽사법재판소의 판결[55]에서 잊힐 권리가 인정되었을 때 관련하여 문제된 쟁점은 청구인이 자신에 관한 기사의 삭제와 구글 검색창에서 검색이 되지 않도록 링크를 삭제해 달라는 것이었다. 즉 제3자의 웹페이지에 공표된 정보추제의 개인정보가 합법적이고 진실한 것이라고 하더라도, 정보 주체가 타인에게 그에 관한 정보가 알려지지 않도록 인터넷 검색엔진이 색인하지 못하거나 검색된 결과의 목록에 웹페이지로 연결되는 링크를 삭제해 달라고 요구할 권리가 있는가가 문제된 것이다.

이에 대해 유럽사법재판소는 유럽연합 기본권헌장 제7조(사생활 및 가족생활의 존중)과 제8조(개인정보의 보호)가 프라이버시권과 개인정보보호권을 인정하고 있고, 검색엔진으로 인해 이들 권리가 침해될 위험이 크다고 보면서, 검색엔진 운영자에게 링크 정보가 개인정보 처리의 목적에 적합하지 않거나 연관성이 없는 경우, 그리고 과도한 경우에는 정보주체가 검색결과의 링크삭제를 요구할 수 있는 권리가 인정된다고 보았다. 이것이 유럽사법재판소가 인정한 이른바 잊힐 권리의 내용이다.

결정 당시에 유럽연합 기본권헌장의 기본권 조항으로부터 삭제권을 포함한 잊힐 권리가 인정될 수 있을 것인지에 대해서는 논란의 여지가 있었다. 당시 유럽연합의 정보처리에 관한 지침에서 정한 정보접근권과 반론권의 해석상 정보처리가 지침을 위반하거나 정보주체의 특별한 상황으로 인해 강한 정당화 사유가 있는 경우 정보주체에게 정정, 삭제, 차단, 반대권을 부여하는 것이지 단순히 해당 정보처리가 자신에게 해가 될 수 있다거나 잊혀지기를 원한다는 이유로 그러한 권리를 부여하는 것이 아니라는 견해도 적지 않았다.

이에 유럽사법재판소는 지침에서 정한 '지침을 위반한 경우'가 해당 정보가 부정확한 경우뿐만 아니라 정보처리목적에 비추어 정보가 부적절하거나, 관련성을 상실하였거나, 과도한 수집, 노후화, 필요이상의 장기간 보유의 경우도 포함된다는 점에 주목하여, 한때 적법하게 수집된 개인정보라도 시간이 지남에 따라 부적법하게 될 수 있다는 점을 지적하였다. 이 점에서 유럽사법재판소의 입장은 EU기본권헌장에 의해 보호받는 정보주체의

55) EuGH, Urteil 13. 5. 2014, Google Spain/AEPD, Rs. C-131/12. 개요는 한동훈, 유럽연합의 잊힐 권리에 관한 연구, 헌법재판연구원 연구보고서 2021, 8-19면을 참조.

기본권이 검색엔진 운영자의 경제적 이익이나 이용자의 정보검색이익에 우선한다고 본 것이다.

유럽연합에서 잊힐 권리를 인정할 당시 잊힐 권리의 의미는 유럽연합기본권 헌장에서부터 직접 도출할 수밖에 없었기 때문에 그 구체적인 내용과 범위는 모호한 점이 있었다. 잊힐 권리는 삭제요구를 넘어 오늘날 디지털 시대에 인터넷 검색엔진에서 검색배제에 대한 청구를 포함하고 있었다.[56] 한편, 유럽연합의 단일한 「개인정보보호법」(GDPR)이 발효(2018. 5. 25.)되면서 이 법 제21조에서 개인정보에 관한 삭제권의 형태로 잊힐 권리를 도입함에 따라 동법에 따른 잊힐 권리는 유럽연합의 모든 회원국에 대해 직접 적용되는 실정법상의 권리가 되었다.

2) 유럽연합과 독일의 판례 발전

독일의 경우에는 연방헌법재판소가 잊힐 권리에 대한 두 차례의 주요한 결정을 한 바 있다.[57]

① 제1차 잊힐 권리(Recht auf Vergessen I)에 관한 결정[58]

주간지인 슈피겔의 온라인 홈페이지(Spiegel Online)의 무료서비스에서 자신이 1982년에 살인을 저질러 무기징역을 선고받고 복역한 사건에 관한 기사가 검색되는 것을 2009년 발견한 청구인은 범죄 검색에서 자신이 검색되지 않도록 법원에 금지청구를 하였다. 주 법원에서는 범죄의 심각성에도 불구하고 시간이 경과되었고 청구인의 범죄가 사람들의 기억에서 사라질 기회를 부여하지 않는다면 청구인의 인격권에 가해지는 침해가 심각하다고 보아 인용하였으나, 연방대법원은 형량 오류를 들어 이를 파기하였다.

이에 청구인은 연방대법원의 판결에 재판소원을 신청하였고 연방헌법재판소는 해당 판결이 기본권으로서의 인격권을 충분히 검토하지 않음으로써 청구인의 인격권을 침해하였다고 결정하였다. 해당 사건에서 청구인이 갖는 일반적 인격권의 제3자적인 효력, 슈피겔 온라인의 일반적 행동의 자유와 언론의 자유, 대중이 갖는 해당 정보 획득에 대한 이

56) 이권일, 위의 논문(2023), 191면 이하를 참조.
57) 관련 개요와 유럽연합의 다층적 권리구제 구조에 대해서는 정문식, 유럽연합 내에서 기본권보장 체계 변화, 유럽헌법연구 제36호, 2021을 참조.
58) BVerfGE 152, 152 - 1 BvR 16/13 (2019. 11. 6. 결정).

익과 시간 경과에 따른 정보 가치의 변화, 디지털 아카이브 구축과 관련한 언론사의 책임 및 의무, 기술 발전에 따른 기술적 조치 가능성 등이 형량 요소로서 주의 깊게 고려되었어야 한다고 판시하였다.

② 제2차 잊힐 권리(Recht auf Vergessen I)에 관한 결정[59]

북독일방송(NDR)은 2010년 기업의 해고를 비판하는 시사프로그램을 내보내면서 텍스트와 함께 이 프로그램을 인터넷 사이트에서 볼 수 있도록 하였다. 이에 따라 해고로 비판받은 기업의 경영자가 자신의 이름이 구글 검색엔진에서 검색되는 것을 발견하자 링크의 삭제를 요청하였고, 이를 거부한 구글을 상대로 주 법원에 삭제를 구하는 청구를 하였다. 주 법원은 6년이 지난 시점에서 판단할 때 여전히 링크를 인정하는 것은 인터넷이용자의 알 권리에도 불구하고 청구인의 인격권 및 정보자기결정권을 침해한 것으로 보았던바, 주 최고법원은 구글의 직업의 자유, 인터넷이용자의 알 권리를 형량할 때 삭제가 타당하지 않다고 보았다.

청구인이 제기한 재판소원에 대해 연방헌법재판소는 앞서 살펴본 제1차 잊힐 권리 결정과 같은 날 내린 다른 결정에서 헌법소원을 기각하였다. 연방헌법재판소가 전개한 논리의 출발은 재판소원에 대한 심사기준이 독일 기본권상의 기본권이 아닌 유럽연합 기본권 헌장의 기본권이라는 것이다. 여기서는 문제되는 구글이 언론사에 해당하지 않기 때문에 링크 삭제 등 금지청구권과 관련된 법적 규율이 전적으로 유럽연합법에 의해 규율되는 영역으로서 독일의 입법자가 개입할 여지가 없다고 보았다.[60]

이에 따라 연방헌법재판소는 유럽연합 기본권 헌장 제7조(사생활과 가족생활의 존중), 제8조(개인정보보호)가 사인에게도 간접적으로 적용될 수 있는 심사기준이 되는 기본권이라고 보고 구글이 가지는 기본권 헌장 제16조의 영업의 자유 및 콘텐츠제공자의 표현의 자유, 인터넷사용자의 정보접근이익을 형량하고 유럽연합의 기본권을 구체화한 개인정보보호법(GDPR)의 보호 내용까지를 포함하여 삭제청구권이 인정되지 않는다고 판단하였다.[61]

---

59) BVerfGE 152, 216 - 1 BvR 276/17 (2019. 11. 6. 결정).

60) 유럽연합의 개인정보보호법 제85조에 따르면 언론사의 경우 개인정보에 대한 특칙을 국가별로 정할 수 있도록 하고 있기 때문에 독일 입법자의 형성재량이 있었다. 이 때문에 제1판결에서는 유럽연합의 기본권 보장 수준에 미달하지 않는 한 독일 기본법상 기본권 보장수준이 심사기준으로서 적용되었다.

61) BVerfGE 152, 216, 256, Rn. 111-122.

3) 시사점

독일연방헌법재판소가 잊힐 권리에 대한 두 결정에서 전개한 논리에는 차별점이 있다. 제2결정에서는 판단의 기준이 유럽연합 기본권 헌장에서 명문화되어 있는 정보자기결정권이었기 때문에 동 기본권과 이를 구체화한 개인정보보호법(GDPR)이 잊힐 권리의 구체적 내용과 적용에 대한 판단의 기준이 되었다.

반면 독일 기본법으로부터 잊힐 권리를 도출한 제1결정에서는 엄격한 의미에서 정보자기결정권이 아닌 일반적 인격권으로부터 잊혀질 권리를 도출한 것으로 이해된다.[62] 즉 정보자기결정권은 새로운 데이터처리 기술의 발달로 인하여 개인정보의 처리 시 정보주체가 모르는 불투명한 정보처리로부터 정보주체를 보호하는 데 적용된다고 한다면, 특정 정보가 투명하게 유포되더라도 자신에 관한 정보가 보도되고 이후 다시 계속 검색되도록 하는 것은 별도로 일반적 인격권으로 보호되는 자기표현권을 제한하는 것이라 구분해 볼 수 있는 것이다.[63] 이에 따라 잊힐 권리의 내용이 추가적인 검색으로부터의 배제를 구하는 권리를 의미한다고 한다면 이는 정보자기결정권과 구분되는 별도의 권리로서의 의의가 인정하기가 더 용이해 진다.

라. 소결

개인정보보호자기결정권이 “자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리”[64]이면서, “타인에게 형성될 정보주체의 사회적 인격상에 대한 결정권을 정보주체에게 유보”[65]시키는 것이라고 한다면, 한국과 독일에서 개인정보자기결정권의 내용은 사실상 동일한 것으로 이해할 수 있다. 다만, 한국 헌법재판소는 개인정보자기결정권을 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권과 헌법 제17조의 사생활의 비밀과 자유을 결합하여 도출하고 있기 때문에, 일반적 인격권으로부터 개인정보보호권을 도출하는 독일과 도출 근거에서는 일정한 차이가 있다고 볼 수 있다.

62) 이권일, 위의 논문(2023), 189면.
63) 이권일, 위의 논문(2023), 189면.
64) 헌재 2005. 7. 21. 2003헌마282등, 판례집 17-2, 81, 90.
65) 헌재 2005. 5. 26. 99헌마513등, 판례집 17-1, 668, 687.

이는 한국의 경우 헌법에 사생활의 비밀과 자유의 불가침에 대한 조항이 있기 때문에 헌법의 조문 내용이 독일과 상이한 데 따른 것이다.[66] 사생활의 자유가 개인이 자신의 사생활을 자율적으로 형성할 자유이며 사생활의 자유를 보호하는 핵심에 개인의 인격에 대한 보장의 취지가 있다고 할 때 구체적인 보호범위에서 사생활의 자유에 대한 보호를 일반적 인격권의 그것과 구분하는 것은 용이한 일이 아니다. 그럼에도 불구하고 사생활의 비밀과 자유의 보호영역으로부터는 보호되지 않으면서 일반적 인격권을 도출 근거로 하여 보호될 수 있는 개인정보자기결정권의 영역이 있다면 인격권으로부터도 같이 개인정보자기결정권을 도출하는 실익이 커질 수 있다.[67] 여기서 사생활의 핵심을 보호하려는 취지에 더해 자유로운 인격 발현을 위한 전제조건으로서의 사적인 인격영역을 보호한다고 보는 독일 관점의 접근은 의미가 있다.[68] 개인정보자기결정권은 디지털화의 과정에서 사회적 인격상에 대한 결정권으로서의 의미가 크기 때문이다.[69] 이는 사생활의 보호에 영향을 미친다고 볼 수 없는 개인정보가 어떤 조건 하에서 기본권적 보호를 요구하는 위험을 초래할 수 있게 되는지의 판단 기준이 될 수 있다. 최근의 빅데이터 정보의 처리나 맞춤형 개인정보 이용, 추천서비스 제공과 관련하여 일상생활에서의 선택과 취향에 대한 제한이 기본권적으로 문제되는 상황을 포착하는 데 개인정보자기결정권의 보호범위가 미칠 수 있을 것이다.

이처럼 인격권으로부터 도출되는 개인정보자기결정권의 보호범위는 사회적 인격상에 대한 자기결정권을 계속적으로 실현해 나갈 수 있도록 하는, 후술할 개인정보에 대한 통제권을 포함하는 것이다. 개인정보에 대한 적극적 통제권을 인정하는 것은 사생활의 비밀에 대한 침해를 막는 측면 외에도 동시에 그 과정에 개인의 사회적 인격상이 고착되는 것을 막는 취지가 함께 있다. 다만, 한편으로 오늘날 개인정보자기결정권은 개인정보가 데이터로서 경제·사회적 가치를 인정받으면서 개인이 자신에 관한 정보의 활용 방식과

66) 전상현, 개인정보자기결정권의 헌법상 근거와 보호영역, 저스티스 제169호, 2018. 12. 22-25면은 독일과 같이 인격권으로부터만 개인정보자기결정권을 도출하는 견해는 물론, 제17조와 함께 제10조를 근거로 제시하는 다수설의 관점에 대해서도 비판적인 견해를 제기한 바 있다. 사생활의 비밀과 자유 또한 자기정보에 대한 통제권을 포괄할 수 있고, 적극적 청구권의 인정 여부 역시 제10조의 인정 여부와 무관하며, 공적 영역에서의 개인정보 또한 “무엇을 보여주고 무엇을 가릴 것인지”를 결정하는 사생활의 비밀과 자유의 핵심에 포괄될 수 있으므로 인격권으로부터의 도출이 필요하지 않다는 것이다.

67) 권건보, 개인정보자기결정권의 보호범위에 대한 분석, 공법학연구 제18권 제3호, 204면 이하는 사적인 정보와 구별되는 개인정보 개념을 설명하면서 개인정보의 경우에는 은닉상태의 유지 여부보다 정보의 자율적 통제에 초점이 있다고 한다.

68) 김일환, 독일 기본법상 ‘일반적 인격권’의 성립과 발전, 법과 정책 제6호, 2000, 15면.

69) 김하열, 헌법강의, 316-317면 이하 참조.

수익분배 방식을 결정할 수 있도록 재산권성을 인정하려 하기도 하는바, 이러한 관점이 통용될 때 그것이 개인정보에 대한 인격권적 위상과 조화될 수 있을 것인가는 쉽게 답하기 어려운 문제일 것이다. 개인정보자기결정권이 사생활 보호나 인격권 보호의 핵심적 가치에 해당하지 않는 영역에 대해서는 그 제한이 사회적 인격상에 대한 침해[70]에 이르지 않는 경우 비교적 넓은 제한의 여지를 열어두고 있다고 이해할 수도 있을 것이다. 이 점에서 우리가 기본권적 차원에서 보호가 필요한 '개인정보'의 의미가 무엇인지는 헌법적 차원에서 다시 한번 숙고해 나가야 한다. 그리고 이러한 신중한 접근 속에서 개인정보에 대한 활용 동의의 문제를 접근해 나가야 할 것이다.

2. 정보기술체계의 신뢰성과 무결성 보장에 관한 기본권

가. 연방헌법재판소의 IT 기본권 결정

독일연방헌법재판소는 일반적 인격권으로부터 정보자기결정권을 도출한 이후 디지털기술 발전에서 흠결될 수 있는 기본권 보장을 위해 다시 이른바 정보기술체계의 신뢰성과 무결성 보장에 관한 기본권(Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer System, IT기본권 또는 컴퓨터기본권이라 불리는데 이하 IT기본권으로 약칭한다)을 도출하여 해소하고자 하였다.

IT기본권이 문제된 사건은 이른바 국가안보 목적의 '온라인 수색'(Online-Durchsuchung)에 관한 사건이었다.[71] 온라인 수색은 '당사자가 모르게 기술적 수단을 통하여 당사자가 이용하고 있는 정보기술시스템에 침입하여 그 시스템에서 데이터를 수집'하는 것을 의미한다. IT기본권 결정은 노르트라인 베스트팔렌주 헌법보호법이 노르트라인 베스트팔렌주의 정보기관인 주헌법보호청의 직무 및 권한에 대해 규정하면서 주헌법보호청에게 온라인 수색의 권한을 인정한 데 대해 위헌 결정을 한 사건이었다.

---

70) 이에 대해, 김하열, 헌법강의, 318면 이하를 참조.

71) BVerfGE 120, 274 - 1 BvR 370/07, 1 BvR 370/07, 1 BvR 595/07 (2008. 2. 27 결정, '온라인수색'결정이라 한다). 동 사건에 대한 개요와 번역으로는 박희영, 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권 (상)/(하), 법제 2008. 10/11을 참조. 해당 판결에 대한 개관으로는, 소은영, 온라인 수색과 헌법상 기본권, 헌법학연구 제29권 제3호, 2023. 9 또한 참조.

연방헌법재판소는 이 사건에서 IT기본권을 일반적 인격권으로부터 도출[72]하였는데, 이처럼 새로운 기본권을 도출한 이유는 개인용 컴퓨터와 전자통신기기와 같은 정보통신기술이 개인의 인격 발현에서 차지하는 중요성이 특별하고 그러한 기술로부터 인격에 대해 발생하는 새로운 위험에 대항할 기본권이 필요하다고 판단하였기 때문이다. 즉 정보기술시스템을 이용하게 되면 의식적으로든 자동적으로든 데이터가 생성되고 저장되며, 그 데이터는 시스템 이용자의 특성과 행동을 추론할 수 있게 하여 개인의 인격을 프로파일링할 수 있게 하는 한편, 해당 시스템이 네트워크로 연결되면 이용자가 대비하거나 의식하지 못한 상태에서 제3자가 그 데이터를 염탐하거나 조작할 기술적 가능성이 열리게 된다. 그런데 이러한 위험에 대비하기 위한 기술적 보호조치는 높은 비용이 들거나 보호시스템의 기능 손실을 감수할 수밖에 없어 시스템에 대한 보호를 간과하기 쉽다. 그러나 제3자가 데이터가 저장되어 있는 시스템에 일단 침입하고 나면 민감한 데이터의 암호화 내지는 은닉 등을 통해 시스템을 보호하려는 시도는 대부분 무력화되게 되며 이를 방어할 기술적 보호장치의 발전도 현실적이지 않다.[73] 연방헌법재판소는 이러한 사정에 대응하기 위해 정보기술시스템에서 발생하는 법익 침해 상황으로부터 포괄적이고 일반적인 인격권 보호를 위한 기본권이 필요하다고 본 것이다.[74]

나. IT기본권의 법리

1) IT기본권의 도출근거와 내용

IT기본권의 보호영역은 시스템에 접근함으로써 개인의 생활상이나 더 나아가 그 개인의 의미 있는 인격상을 들여다볼 수 있게 하는 개인 관련 데이터를 담고 있는 독자적·네트워크화된 시스템이다. 여기에는 개인 데이터를 담고 있는 이동전화나 전자수첩도 해당될 수 있다.[75] 정보기술 시스템 그 자체의 이용을 감시하거나 시스템의 저장매체를 수색하는 경우가 IT기본권에 대한 전형적인 권리 제한의 상황이다.[76] 이처럼 IT기본권은 일종의 사생활의 영역 개념으로서 정보기술시스템을 보호하면서 시스템이 생성·처리·저장

72) BVerfGE 120, 274, 303 (Rn. 168 ff).
73) BVerfGE 120, 274, 306.
74) BVerfGE 120, 274, 306 이하.
75) BVerfGE 120, 274, 314 (Rn. 203).
76) BVerfGE 120, 274, 308 (Rn. 186).

하는 데이터의 신뢰성과 시스템의 신뢰성과 무결성 자체를 보호하는 것이다. 즉 보호의 대상인 정보기술시스템으로 생성, 처리, 저장되는 데이터의 비밀을 유지하고 제3자가 그 시스템에 침입하여 시스템의 성능, 기능 또는 저장내용을 이용하지 못하도록 하여 정보기술시스템이 무결하게 유지되는 이익을 보호한다는 것이다.[77]

이는 개인용 컴퓨터, 전기통신장치나 주거 및 자동차에 포함된 전자적 장치들이 이용됨에 따라 인격의 발현을 위한 정보기술에 대한 보호의 중요성이 나날이 커져가고 있고,[78] 정보기술 시스템이 전산망으로 연결하여 네트워크화됨으로써 개인용 컴퓨터 자체의 기능이 네트워크를 통해 확장되는 현상에 주목한 결과이다.[79] 이러한 권리의 보장 필요성은 오늘날 사물인터넷 등이 발달하고 사회적 인프라가 디지털화하면서 더 중요하게 되었는데, 이른바 스마트시티나 자율주행자동차 운영을 위한 인프라의 안전시스템을 보호할 필요성이 더욱 커진 것이다.[80] 여기에는 개인용컴퓨터, 네트워크, 인터넷, 모바일기기, 마이크로칩, 스마트카드 외에 스마트 주거(Intelligente Wohnungen)의 가전제품이 망라될 수 있다.[81] 개인과 개인, 개인과 사물이 연결된 네트워크에서 이른바 '가상의 주거'(virtuelle Wohnung)가 있다면 이러한 '전자적 의미에서의 사적영역'(elektronische Privatsphäre)에 대해 보호하는 것은 '개인정보보호'의 범위를 넘어서는 것[82]으로서 네트워크의 보호는 소통에 대한 보호의 의미를 함께 가질 수 있다.

여기서 정보기술시스템에 대해서 보호하고자 하는 것은 신뢰성과 무결성이다. 시스템의 신뢰성이라는 것은 시스템의 신빙성에 의해 포괄되는 개념들이다. 즉 보호하고자 하는 정보기술에서의 안전(Sicherheit in der Informationstechnik)은 신빙성(Verlasslichkeit)과 통제가능성(Beherrschbarkeit)을 포괄한다. 즉 신빙성은 필요한 경우 언제든지 작동가능해야 한다는 작동가능성(Verfügbarkeit), 권한이 있는 사람만이 작동할 수 있다는 신뢰성(Vertraulichkeit), 그리고 권한이 없는 사람에 의한 조작이 없었다는 무결성(Integrität)을 포괄한다. 또 통제가능성은 시스템이 불측의 피해로 손상을 입지 않는다는 것을 보증하는 제어성, 시스템의 프로세스가 어떤 방식으로 작동하는지를 파악할 수 있다는 귀속성(Zurechenbarkeit), 문제시 법적으로, 제3자에게 프로세스와 데이터를 제시할 수 있다고

77) BVerfGE 120, 274, 314 (Rn. 204).
78) BVerfGE 120, 274, 304 (Rn. 173).
79) BVerfGE 120, 274, 304 (Rn. 175).
80) Hauser, Das IT-Grundrecht. Schnittfelder und Auswirkungen, 2015, 66-67면.
81) 상세히는, Heinemann, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, 55-69를 참조.
82) Hauser, 위의 책, 67면.

하는 법구속성(Rechtsverbindlichkeit)을 모두 포함한다고 한다.[83] 이처럼 정보시스템에 대한 다양한 기대를 담아 연방헌법재판소는 IT기본권을 적용함으로써 "정보기술시스템이 공격을 받아서 그 성능, 기능 및 저장매체의 내용이 제3자를 통해서 이용되지 않도록 보호해야 할 정보기술시스템의 무결성이 침해되는지 여부를 판단하고 통제가능성을 확보하도록 한다. 따라서 구체적인 데이터를 수집하도록 시스템에 접근하였는지 여부는 중요하지 않다. 이러한 점은 IT기본권이 정보자기결정권이 수행하는 기능과 차이를 낳는 점이다. 그리고 정보자기결정권은 데이터 수집 및 처리를 보호하는 것인 반면, 온라인 수색에서 '기술적 수단'(감시소프트웨어)의 투입으로 IT시스템에 대한 접근가능성이 열리게 되면 이미 그 때부터 IT기본권은 제한되는 것이다.

IT기본권이 인격권에서 도출되는 것이기는 하지만 사생활권이나 정보자기결정권과 다른 점은 개인정보뿐만 아니라 모든 데이터에 대한 접근에 적용된다는 점이다.[84] IT기본권은 사생활이나 인격에 대한 위험이 문제되는 정보자기결정권이 적용되는 단계 이전에서 작동한다. IT기본권은 개인의 정보 자체를 직접 건드리지 않더라도 시스템에 접근하는 순간, 데이터 수집이나 데이터처리 조치를 위임받지 않고서도, 데이터 전반에 접근이 가능하게 되기 때문에 이는 당사자의 인격에 미치는 영향의 중요성에서 개별적 데이터 수집에 의한 기본권 제한과는 질적인 차이가 있다.[85] 즉 자신의 인격을 담은 시스템을 국가기관이 감시하지 않는다는 전제에서 아무런 두려움 없이 자신을 표현할 수 있는 것은 사생활 형성의 핵심영역에서 인격 발현을 보호하는 것이다.[86] 특히 정보기술시스템은 개별 주체의 개인정보 외에도 스스로 개인과 관련한 데이터를 독자적으로 생산할 수 있는데 이렇게 생산된 정보가 외부에 의해 수집되고 평가되는 것 역시 개인의 인격을 추론하고 그 특징을 프로파일링하게 하는 것이 될 수 있다.[87]

오늘날 인터넷을 통해 시스템이 네트워크화되는 것은 시스템에 있는 데이터에 대해 제3자가 접근할 가능성을 확대하지만 개인이 이에 대해 개입하여 통제권을 행사하기가 어렵다.[88] 여기서 개인이 가지는 통제권은 국가에 대한 것이기도 하다. 개인은 정보시스템을 익명성을 보장받으면서 이용할 수 있어야 한다는 의미를 포함하는데, 그러한 익명

83) Heinemann, 위의 책, 73-78면을 참조.
84) BVerfGE 120, 274, 311 (Rn. 196 ff).
85) BVerfGE 120, 274, 313 (Rn. 200).
86) BVerfGE 120, 274, 335 (Rn. 271); BVerfGE 109, 279, 314.
87) BVerfGE 120, 274, 305 (Rn. 178).
88) BVerfGE 120, 274, 306 (Rn. 180).

성 보장의 어두운 면에 대한 통제를 위해 국가의 개입을 정당화하고자 하는 경우에도 투명한 개입을 보장하여 개인의 통제가능성을 보장하기 위해 IT기본권이 요구된다.[89]

정보기술 시스템 이용자는 데이터가 자신의 사생활에 대한 데이터가 아니라고 하더라도 시스템이 침입에 의해 자신의 사생활에 해당하지 않는 데이터로부터 자신의 인격에 영향을 미치는 제한이 발생할 수 있다. "데이터가 당사자에게 어떠한 의미를 가지는가 그리고 다른 관련성을 고려하여 어떠한 의미를 얻을 수 있는지는 데이터 자체로부터 평가할 수 없"[90]기 때문이다. 이처럼 IT기본권은 구체적 위험의 전 단계에서 인격을 보호하는 기능을 한다. 적은 정보에 의해서도 정보 접근의 목적과 기존 정보와의 결합가능성에 의해 중대한 기본권적 영향이 발생할 수 있다.[91] 따라서 IT기본권은 개인의 통신 과정이나 저장 데이터에 침입하는 것만이 아니라, 전체 정보기술 시스템에 침입하는 것으로부터의 보호를 꾀한다.[92] 즉 "시스템이 그 시스템만으로 또는 그 시스템을 기술적으로 네트워크화해서 개인정보가 포함될 수 있게 되는 경우, 시스템에 대한 접근이 개인의 사적 생활 형성에의 중요한 부분을 보게 하거나 인격에 대한 풍부한 표상을 획득할 수 있게 하는" 위험을 막아야 하기 때문이다.[93]

2) 정보기술시스템의 적용례

가) 연방범죄수사청법의 온라인 수색

IT기본권의 경우 온라인 수색을 허용한 조항에서 그 기본권 침해여부를 심사하는 기본권으로서 문제되는 기본권을 기능을 하였다. 이후 연방범죄수사청법의 온라인 수색 사건에서에 국제테러의 위험을 방지하기 위하여 연방범죄수사청법(BKAG)에 다양한 비밀감시조치들을 도입한 법률이 문제된 경우에도 IT기본권은 등장하였다.

이 사건에서는 온라인 수색을 포함하여 주거 내 음성 감시, 전기통신감청, 통신사실 확인자료 수집, 데이터를 수집하기 위한 특별한 수단을 사용한 주거 외 감시와 온라인 수색에 관한 규정이 포함되어 있었다. 온라인 수색에 대해서는 IT기본권 결정에서 연방헌

89) Heinemann, 위의 책, 80면.
90) BVerfGE 120, 274, 311 (Rn. 197).
91) BVerfGE 118, 168 - 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05 (2007. 6. 13. 결정).
92) BVerfGE 120, 274, 313 (Rn. 201).
93) BVerfGE 120, 274, 314 (Rn. 203).

법재판소가 제시한 기준에 따라 연방범죄수사청법 제20k조에 온라인 수색에 관한 조항을 마련하였던 것이다.[94] 즉 독일 연방범죄수사청법은 '정보기술시스템에 대한 비밀침입'이란 표제 하에서 국제테러의 위험을 방지하기 위하여 테러와 관련한 특정한 위험이 존재하는 경우 "당사자 모르게 기술적 수단을 통하여 당사자가 이용하고 있는 정보기술시스템에 침입하여 데이터를 수집할 수 있다."고 규정하는 근거조항을 두었다(제20조k).

이에 대해 연방헌법재판소는 비밀감시조치와 관련한 수권조항들 중 사생활의 핵심영역의 보호에 관한 규정은 헌법에 합치하지 않는다고 결정하였다.[95] 즉 연방헌법재판소는 문제된 조항이 IT기본권을 제한하는데,[96] 온라인 수색에 대한 실질적·절차적 요건에 관한 조항이 헌법원칙과 비례원칙 차원에서 충분하지 않다고 판단하였다.[97] 정보기술시스템에 대한 비밀 접근으로 고도의 비밀성이 있는 데이터가 수집될 위험이 있는 상황에서 사생활의 핵심영역의 보호를 위해 명백한 법률상 보호조치들이 있는 경우에만 기본권적 요청이 충족될 수 있다는 것이다. 연방헌법재판소는, 사생활의 핵심영역에 관한 데이터를 수집하는 것이 처음부터 완전히 금지되는 것은 아니지만, IT기본권은 전체 데이터베이스에서 디지털 데이터로 존재하는 고도의 비밀스런 정보가 읽혀지지 않도록 보호하는 데 목적을 두어 기본권적인 평가가 필요하다고 보았다.[98]

따라서 기본권 핵심영역의 보호에 관한 요구사항이 수집단계에서 어느 정도 완화될 수 있다고 하더라도 이에 대해 특별히 유효한 정보 기술적 보호조치가 마련되어야 하며, 만약 기술적 보호조치로 인해 고도의 기밀정보가 탐지되고 분리될 수 있다면 그 영역에 대한 접근 자체를 중단시켜야 한다고 한다.[99] 반면 핵심영역 관련 데이터가 데이터수집 이전에 또는 수집 시에 분리될 수 없다면, 고도의 인격적 관련성을 가진 데이터가 추가로 수집될 개연성이 존재하는 경우에 정보기술시스템 접근을 허용하되 그러한 접근으로 인한 영향을 최소화해야 한다고 한다. 그리고 이러한 결정에서의 독립성, 즉 연방범죄수

94) 테러방지를 위한 연방범죄수사청법의 개정에 대해서는 박희영, 독일 연방사법경찰청에 의한 국제테러의 위험 방지를 위한 법률(상), 법제처, 법제 제613호, 2009. 1, 20-43; (하), 법제처, 법제 614호, 2009. 2, 16-25면을 참조.

95) BVerfGE 141, 220 - 1 BvR 966/09 (2016. 4. 20. 결정, '연방형사청법 결정'이라 한다). BVerfG 141, 220, 306. 관련 소개로, 이상학, 테러방지 수권규정과 기본권 침해의 한계, 공법학연구 제17권 제3호, 2016. 8.; 박희영, 최근 독일 정보기관의 정보수집권 확대와 형사정책적 시사점, 형사정책연구 제32권 제3호, 2021. 9.을 참조.

96) BVerfGE 141, 220, 303 (Rn. 209).

97) BVerfGE 141, 220, 304 (Rn. 211).

98) BVerfGE 141, 220, 306 (Rn. 218).

99) BVerfGE 141, 220, 307 (Rn. 219); 온라인 수색결정, Rn. 281.

사청이 아닌 독립기관에 의해 사전에 이러한 접근의 허용 여부를 결정하는 것이 중요하다고 보았다.[100]

이러한 기준에 따라 연방헌법재판소는 연방범죄수사청법(BKAG) 제20k조 제7항에서 데이터 수집 및 사용 단계에서의 핵심영역보호에 대해 판단하였다. 이에 따르면 데이터 수집단계의 규정(제7항 제2문)은 헌법에 합치하는데,[101] 핵심영역의 데이터가 수집되지 않도록 모든 기술적 가능성을 이용해야 하고 사생활 형성의 핵심영역의 데이터만 수집될 경우에는 정보기술시스템에 대한 접근이 금지된다고 정하고 있었기 때문이다. 반면 수집된 데이터의 열람 및 분석 단계의 규정들(제3문, 제4문)은 핵심영역의 보호가 충분하지 않다고 보았는데, 특히 독립적인 기관에 의해 수집된 데이터의 열람이 이루어져야 하지만 이에 대한 통제가 마련되어 있지 않다고 본 것이다. 이에 해당 규정은 수집된 데이터에 대한 열람 및 분석 권한을 연방범죄수사청의 직원에 맡기고 있기 때문에 헌법에 합치하지 않는다고 판단하였다.

나) 형사소송법에서의 범죄 수사 목적의 온라인 수색

한편 테러범죄에 관한 수사를 위해서 형사소송법의 규정(제100b조, 제100d조, 제100e조, 제101조)에 따른 온라인 수색을 실시할 수도 있도록 한 조항 또한 문제되었다. 형사소송법은 온라인 수색의 요건으로, 첫째, 누군가가 정범 또는 공범으로 '특별히 중한 범죄'를 범했거나 가벌적 미수 사례에서 미수를 범하였다는 혐의를 특정한 사실이 뒷받침하고, 둘째, 특별히 중한 범죄행위가 있었으며, 셋째, 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 본질적으로 어려울 수 있거나 가망이 없는 상황을 제시하고 이를 충족할 경우 온라인 수색을 실시할 수 있다고 하고 있다.

이와 관련하여 연방헌법재판소는 범죄수사 목적의 온라인 수색(형사소송법 제100b조 이하)에 대해서는 아직 판단을 내리지 않은 상태이다. 연방헌법재판소는 이미 IT기본권의 제한은 범죄의 예방적 목적뿐만 아니라 형사소추를 위해서도 정당화될 수 있다고 보았기는 하나[102], 이에 대한 헌법소원은 여전히 계속중에 있다.[103] 조항에는 온라인 수색 외에 통신종료 후 정보기술시스템에 침입하는 암호통신감청(형사소송법 제100a조 제1항

100) BVerfGE 141, 220, 307 (Rn. 220).
101) BVerfGE 141, 220, 307-308 (Rn. 222).
102) 온라인수색 결정, Rn. 207; 박희영, 독일 연방헌법재판소의 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 법무부, 인터넷법률 통권 제45호, 2009. 1, 114
103) 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18.

제3문)에 관한 내용이 포함되어 있다(형사소송법 제100a조 제1항 제2문과 제3문). 특히 형사소송법은 앞서 법령과 달리 온라인 수색이 가능한 특별히 중한 범죄에 소유권이나 재산권과 같은 법익의 침해에 대해서도 온라인 수색을 허용하고 있는 점에서 논란이 되고 있다.

다. 디지털 전환의 안전장치로서 IT기본권

1) 개인정보자기결정권과의 차별성

연방헌법재판소가 IT기본권을 정립하였음에도 불구하고 이 기본권의 독자적 성격에 대한 의문이 지속적으로 제기되었을 뿐만 아니라 해당 기본권이 이후의 헌법재판소 결정에서 적극적으로 적용되고 있는 것은 아니라는 지적도 있다. 최초 IT기본권의 선언 이후 상당한 기간 동안 IT기본권이 활용되지 않아 언론에 '잊혀진 기본권'이라는 지적을 받기도 하였기 때문이다.[104]

IT기본권은 정보자기결정권이나 기본법 제10조(편지·우편 및 통신의 비밀), 제13조(주거의 불가침)의 자유 보장과는 독립된 권리임을 IT기본권 결정 당시부터 제시한 바 있다. 그에 따르면 정보기술 시스템에 비밀리에 접근하는 행위는 통신의 자유에 대한 제한에 포괄될 수 없는데, 저장되어 있는 컴퓨터의 자료에 접근하는 경우에는 통화중인 상태에서의 정보접근에서 문제되는 통신의 자유와 무관한 것이기 때문이다. 주거의 불가침 보호와도 IT기본권은 "사생활을 발현하는 공간적 영역을 보호하는 것"[105]과는 일정한 차이가 있다고 한다. 이 기본권은 공간과 무관하게 휴대용 컴퓨터나 스마트폰에 대한 침입에 적용될 수 있다.

특히 데이터의 신뢰성을 보호하는 것과 관련하여 이는 정보자기결정권의 문제로 해소할 수 있고 별도로 IT기본권이 필요한가에 대해 의문이 제기되기도 하였다.[106] 이에 대해 연방헌법재판소는 개인정보자기결정권은 개인의 개별적인 데이터 수집에 대해서만 보호하지만 IT기본권은 시스템에 대한 침입으로 대규모의 의미있는 데이터 세트가 획득될

104) Baum/Kurz/Schantz, Das vergessene Grundrecht, Frankfurt Allgemeine Zeitung, 2013. 2. 26.
105) BVerfGE 120, 274, 309 (Rn. 192).
106) Eifert, Informationelle Selbstbestimmung im Internet, NVwZ 2008, 521 참조. 우리나라의 경우에도, 소은영, 온라인 수색과 헌법상 기본권, 헌법학연구 제29권 제3호, 2023. 9. 64면은 사생활의 비밀과 자유의 침해로 보는 것이 적절하고, 온라인 수색으로 인한 침해 양상의 특수성을 감안하여 그 침해 여부를 판단하는 것이 간명하다고 보고 있다.

수 있는 점에서 별도의 취급이 필요하다는 관점을 취한 것으로 보인다. 개인이 인격발현을 위해 정보기술시스템의 이용에 의존하고 있지만, 이 시스템에 인적 정보가 들어있거나 반드시 이 시스템의 이용을 통해서만 전송되는 경우로부터 발생하는 인격권만이 문제되는 것은 아니기 때문에 독자적인 의미가 있다고 할 수 있다는 것이다. 반면 이에 대해서도 데이터 수집을 통한 정보자기결정권에 대한 제한 또한 데이터 수집의 양과 질, 기간에 따라 그 강도가 다르므로 IT기본권과 본질적인 차이가 있다고 보기는 어렵다는 비판도 있다.[107] 개인정보자기결정권 역시 사전적인 자동적인 처리의 단계에서 이미 개인정보가 제한되는 문제를 포괄할 수 있다고 보아 확장 적용할 수 없는가 하는 의문도 제기될 수 있다. 이것은 결국 개인정보자기결정권의 보호영역 확장을 통해 해결할 것인지의 선택의 문제이다.[108]

시스템에 대한 보호의 필요성은 무엇보다 개인이 이 시스템을 통제할 수 없다는 데 있다. 개인이나 기업은 자신의 정보가 어떻게 이용, 남용되고 있는지 알기 어렵기 때문에 이러한 시스템의 안전을 국가가 제한할 경우 이를 통제하고 더 나아가 국가가 안전을 '보장'하도록 요구할 기본권이 '안전'한 생활을 위한 전제로서 중요하게 된 것이다. 국가가 시스템에 침입하는 경우는 물론 해킹 조작 등의 위험으로부터 시스템을 보장하도록 요구할 권리가 IT기본권에는 포함된다.

IT기본권이 보호하고자 하는 기본권적 문제상황은 오늘날 개인의 기본권 보호에 대한 문제상황이 순수히 개인에 귀속되는 정보에 대한 보호의 위험을 넘어 자신과 직접적인 관련성이 없는 정보체계에 대한 위험으로부터도 초래될 수 있다는 점을 보여 준다. 즉 '새로운' 복잡한 정보기술 체계가 초래하는 사회적 위험에 대한 보호를 기본권의 이름으로 천명하고 사회적 위험으로부터의 보호를 개인의 기본권적 이익으로서 평가되도록 할 필요가 있다는 것이다. 기본권의 의의와 기능을 이렇게 확장하는 것은 디지털 전환으로 대변되는 정보기술의 발전이 초래할 위험에 대한 대응의 특징적인 상황을 보여준다.[109] 이러한 IT기본권의 포괄적이고 보충적인 성격은 디지털 전환과 정보통신기술의 발전을 통해 발생하는 기본권 보장의 공백을 해소할 수 있는 기본권으로서의 위상을 가질 수 있다. 이러한 성격의 IT기본권이 어떤 구체적 권리로서의 성격을 가질 수 있을 것인지 우리 헌법 체계 내에서 검토가 필요한 이유이다.

---

107) Rixen, Kommentar, Art. 2 GG Rn. 73d.
108) 계인국, 인터넷 검색엔진과 개인정보보호, 법제연구 46호, 2014, 172면.
109) Kloepfer/Schärdel, Grundrechte für die Informationsgesellschaft, JZ 2009, 453.

2) 객관적 가치질서 차원의 IT기본권

IT기본권의 의미는 '개인정보'의 보호범위에 해당하지 않는 '시스템'의 안전에 대해 기본권을 인정한 것으로서, 이러한 시스템 보호를 위한 기본권의 인정이 주관적 권리로서의 성격을 가질 수 있는가에 대한 의문이 제기될 수 있다. 법리적으로 자유권적 기본권의 보장이 객관적 질서의 보장이기도 하다고 보더라도 IT기본권의 핵심적 기능은 IT기본권의 법익을 보호하는 것이 국가의 의무라는, 객관적 가치질서 보장의 측면이 강조되지 않을 수 없다.

따라서 IT기본권이 실제 헌법재판에서는 적극 활용되지 않았다고 하더라도 이에 대한 헌법재판소의 기준 제시는 관련 입법의 기준으로서 의미가 적지 아니하다. 즉 온라인 수색과 암호통신감청에 관한 형사소송법 개정의 내용은 IT기본권의 내용을 구현한 것으로서 기본권의 객관적 가치질서 보장의 의미를 살린 것이라 평가하기도 한다.[110]

이 점에서 IT기본권을 헌법상 기본권으로 인정하는 실익은 IT기본권이 보호하고자 하는 법익이 헌법질서에서 차지하는 중요성을 강조하는 데 있는지도 모른다. IT기본권의 정식 명칭이 정보기술시스템의 신뢰성과 무결성의 '보장'에 관한 기본권이라는 점을 상기한다면 IT기본권의 중심에는 국가에 의한 기본권 '침해'보다 보장에 대한 '책임'이 중심에 있다고 할 수 있다.[111] 이러한 객관적 가치로서의 측면은, IT기본권이 기본권적 차원으로 보장되는 법익의 보호를 위한 보호의무 인정, 전체 법질서에 미치는 방사적 효력, 조직과 절차를 통한 형성 요청, 제도적 보장이라는 차원에서 의미를 가질 수 있다.[112]

사이버공간에서의 안전에 관한 기본권은 결국 IT인프라에서의 안전을 국가가 보장해야 한다는 보호의무로 연결된다.[113] 따라서 IT기본권은 국가가 인프라의 안전을 감독하는 취지가 아니라 이를 '보장'하는 책임을 지는 것으로 이어진다. 안전한 정보기술체계의 지원과 이를 위한 입법의 완비는 국가의 보장책임의 내용에 포함될 수 있다.

---

110) Buermeyer/Moini, Gute Lücken, schlechte Lücken? Zur objektiv-rechtlichen Dimension des IT-Grundrechts, Verfassungsblog 2018. 9. 8.

111) Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009, 1019면. 물론 이러한 측면은 주관적인 권리로 IT기본권을 구성하는 것에 대한 비판의 지점이기도 하다.

112) Heinemann, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, 209면 이하; Hauser, Das IT-Grundrecht, 2015, 290면 이하를 참조.

113) 같은 취지로, 김태오, 사이버안전의 공법적 기초: 독일의 IT-기본권과 사이버안전법을 중심으로, 행정법연구 제45호, 121면 이하.

이러한 기본권의 방사적 효력은 계약관계나 노사관계에서도 시스템 안전에 대한 요구를 이해관계의 균형을 고려하며 반영할 것을 요구하는 의미를 가질 수 있으며,[114] 적어도 사이버 공간에서의 안전을 확보하기 위한 조직과 절차을 갖출 의무를 포함한다.

3. 유럽연합의 디지털 전환 입법과 새로운 권리의 제도화 모색

가. 유럽연합의 디지털 전환 관련 주요 법률과 디지털 권리

1) 「유럽연합 개인정보보호법」의 디지털 권리

가) 프로파일링 거부권 등

2018. 5. 발효된 「유럽연합 개인정보보호법」(이하 'GDPR'이라 한다)[115]은 디지털화된 정보에 대한 망라적인 입법적 규율로 평가된다. 이 법 제3장은 특히 정보주체의 접근권, 정정권, 삭제권, 처리제한권은 물론 데이터이동권, 반대권, 프로파일링 거부권 등까지 개인정보보호에 관해 망라적인 규율을 담고 있다. 이 중에서 삭제권은 앞서 본 '잊힐 권리'의 법제화(법 제17조)로 평가할 수 있다. 개인정보보호법은 디지털 시대의 권리로서 삭제권 외에도 데이터이동권, 알고리즘[116] 등에 의한 프로파일링 거부권을 비롯한 자동화된 의사결정에 대한 권리를 인정하고 있는데, 이는 지능정보기술에 대한 디지털 권리의 보장이라는 차원에서 의미가 크며, 최근 한국의 「개인정보보호법」 개정은 GDPR로부터 많은 영향을 받았다.[117] 이 권리들의 개별적인 내용에 대해 상론하기는 어려우므로 이하에

114) Heinemann, 위의 책, 2015, 214-216면 이하 참조.

115) VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

116) '알고리즘'을 명확히 법적으로 정의내리기는 어려우나, 입법안 중에는 '어떤 문제의 해결 혹은 의사결정을 위하여 입력된 자료를 토대로 결론을 이끌어내는 연산 또는 논리의 집합'으로 정의한 것이 있다(이원욱 의원 발의 「지능정보화 기본법」 개정안, 2021. 4. 30. 의안번호:2109836).

117) 2024. 3. 15. 시행되는 「개인정보보호법」은 CCTV와 같은 고정형 영상정보처리기기 외에 드론, 자율주행 자동차 등을 이용한 이동형 영상정보처리기기에 대한 규율을 추가하고(제2조 제7호의2 및 제25조의2 참조), 특히 인공지능 기술을 적용한 시스템을 포함하는 자동화된 시스템으로 개인정보를 처리하여 이루어지는 결정이 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에는 해당 결정을 거부하거나 해당 결정에 대한 설명 등을 요구할 수 있도록 하는 규정을 개설하였다(제4조 제6호 및 제37조의2). 이에 대해서는 후술하기로 한다.

서는 GDPR에서 구체화된 권리가 갖는 헌법적인 위상의 관점에서 프로파일링에 대한 반대권과 자동화된 개별 의사결정에 대한 권리의 내용을 살펴보기로 한다.[118]

특히 “개인의 일정한 개인적 측면을 평가하기 위해, 특히 업무능력, 경제력, 건강, 선호도, 관심사, 행태, 위치 또는 이동 경로 등을 분석하거나 예측하기 위하여 행해지는 모든 형태의 자동화된 개인정보 처리”(GDPR 제4조 제4항)를 가리키는 ‘프로파일링’은 앞서 예측적 경찰활동을 위한 데이터베이스 활용 관련 독일 연방헌법재판소의 결정[119]에서와 같이 인물 추적 등을 위한 용도는 물론 특히 민간 영역에서 개인의 취향을 분석하여 맞춤형 광고 등을 통해 마케팅의 효율성을 높이는 용도로 활용되고 있다. 그러나 자동화된 형태로 개인정보를 처리하는 프로파일링이 개인에 대한 ‘평가’, 특히 분석 및 예측에 사용되는 경우 이는 인간의 존엄성과 자율성에 대한 심각한 위협을 초래할 수 있기 때문에 개인은 프로파일링에 대한 통제권을 가질 필요가 있다.[120] 이러한 이유로 GDPR은 프로파일링을 거부할 권리를 명문으로 인정하고 있다(제21조). 이에 따르면 프로파일링이 공익적 목적이나 공공기관의 임무 수행을 위한 경우 또는 개인정보처리자의 정당한 우월적 이익을 위한 경우에 정보주체가 자신의 특수한 사정을 들어 프로파일링에 반대할 권리를 가진다. 다만, 개인정보처리자가 정보주체의 권익과 자유에 우선하는 처리를 위하여, 그리고 소송의 제기와 방어를 위하여 강력한 정당화 사유를 입증하는 경우에는 프로파일링을 계속할 수 있다(제21조 제1항). 한편 직접 마케팅을 목적으로 개인정보가 처리되는 경우에도 정보주체는 마케팅을 위해 자신에 대한 프로파일링을 하는 것에 대해 반대할 권리를 가지며 정보주체의 의사에 반하여 개인정보처리자가 개인정보처리를 계속할 수 없다(제21조 제2항).

GDPR은 자동화된 의사결정과 관련하여 정보주체의 정보를 정보주체로부터 개인정보처리자가 획득할 때(제13조 제2항 f호, 제14조 제2항 g호) 및 정보주체의 정보를 개인정보처리자가 획득할 때(제15조 제1항 h호) 공정한 정보하고 투명한 처리를 위하여 추가적인 정보를 제공하도록 하고 있기도 하다. 즉 프로파일링 등 자동화된 의사결정을 할 때 ‘처리의 중요성과 예상되는 결과’, ‘사용되는 로직’에 대해 알리도록 한 것이다. 그리고

118) 개관으로, 김재완, EU 일반정보보호규정(GDPR)의 알고리즘 자동화 의사결정에 대한 통제로써 설명을 요구할 권리에 대한 쟁점 분석과 전망, 민주법학 제69호, 2019. 3; 권건보, 지능정보시대에 개인정보자기결정권의 실효적 보장방안, 미국헌법연구 제30권 제2호, 2019. 8, 19면 이하를 참조.

119) BVerfGE 2022. 4. 26 - 1 BvR 1619/17, 본 보고서 20면 이하 참조.

120) 권건보, 위의 논문, 24면.

앞서 본 바와 같이 프로파일링을 포함한 자동화된 의사결정이 중요한 권리의무에 영향을 미치는 경우에는 자동화된 의사결정 자체에 대해 정보주체의 거부권을 명문으로 정함으로써 정보주체의 통제권을 보장하고 있다.

나) 자동화된 의사결정에 대한 권리

이상의 권리가 자동화된 의사결정 이전에 정보주체가 갖는 권리라면, 자동화된 의사결정 이후에는 정보주체가 자신에 관한 법적 효력을 낳거나 자신에게 중대한 영향을 미치는 결정이 프로파일링 등 사람의 개입없이 자동적 정보처리에만 근거하여 이루어질 때 그 결정의 적용을 받지 않을 권리를 가진다(제22조).[121] 이는 프로파일링을 포함해 자동화된 정보처리에 의해 의사결정이 이뤄질 경우 인간이 자신의 삶을 자율적으로 결정하는 주체성에 손상을 입을 수 있다고 보기 때문이다. 이에 개인정보처리자는 이를 막는 적절한 안전조치의 이행을 위해 자동적 정보처리에 대해 구체적인 설명을 들을 권리, 인간의 개입을 요구할 권리, 자신의 관점을 표현할 권리, 자동화된 심사에 따른 결정에 대해 설명을 들을 권리, 해당 결정에 대해 이의를 제기할 권리 등을 보장할 적절한 보호조치가 마련되어야 하며, 공정하고 명백한 개인정보처리를 정보 주체에게 보장하기 위하여 개인정보처리자는 개인정보가 처리되는 특수한 상황과 맥락을 고려하여 프로파일링을 위한 적절한 수학적 또는 통계적 절차를 사용하여야 하고, 특히 개인정보에 오류를 초래하는 요소들이 수정되고 오류의 위험이 최소화되도록 필요하고 적절한 기술적·조직적 조치를 적용하여야 한다고 한다.[122] 이러한 취지에 따라 GDPR 제22조 제3항으로부터 정보주체는 자동의사결정에 대해 정보처리자 입장에서 개입할 권리, 자신의 관점을 표현할 권리, 자동화된 의사결정에 대한 이의를 제기할 권리를 가진다(이를 묶어 정보주체의 갖는 '인간의 개입권'이라고 한다[123]). 인간의 개입권을 규정한 것은 그 실효성 여부와 별개로 적어도 인간의 주체성과 관련한 결정에 대해서 기계에 의한 일방적 결정권을 인정하지 않겠다는 인간 존엄성의 선언이라고 설명된다.[124] 이러한 권리는 인격권으로서 개인정보자기결정권이 사회적 인격상에 대한 통제력을 확보하는 것이라는 차원에서 개인정보자기결

121) 한국「개인정보보호법」제37조의2의 내용도 유사한 취지이다. 정보주체에게 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에 한하여 이를 거부하고 설명, 인적 개입에 의한 재처리를 요구할 수 있도록 한다. 일정한 예외에 해당하는 경우 거부권은 배제된다.

122)「유럽연합 개인정보보호법」(GDPR) 입법이유 71 참조.

123) 김희정, 알고리즘 자동의사결정으로부터 개인의 보호, 헌법학연구 제26권 제1호, 2020. 3. 222-224면 참조.

124) 김희정, 위의 논문, 226면.

정권의 내용에 포괄되는 것으로 이해할 수 있다.[125]

한편 설명요구권을 포함하는 인간의 개입권은 알 권리를 그 근거로 삼기도 한다. 이는 표현의 자유 차원에서 자유로운 의사의 형성은 충분한 정보에의 접근이 보장됨으로써 가능하고 알고리즘 정보에 대한 접근 가능성 보장은 그러한 실질적 권리보호의 전제를 충족시키는 기능이 있다는 것이다.[126]

디지털 시대의 알 권리에는 정보원으로부터 방해없이 정보를 받을 수 있는 정보수령권도 포함될 수 있다.[127] 알고리즘에 의해 자신이 추천받는 정보 위주로 정보를 접하고, 자신과 유사한 견해에 갇히게(필터 버블 현상)될 때[128] 알 권리에서 도출되는 정보수령권은 디지털 기술에 대한 통제권으로서의 의미를 가질 수 있다. 이러한 권리는 정보선택의 자유, 정보노출의 다양성 및 투명성 등의 보장을 내용으로 한다.[129] 이러한 알 권리는 오늘날 알고리즘의 불투명성이 가져올 차별의 가능성을 해소하기 위해서도 필요하다. 빅데이터에 의한 알고리즘은 그것이 불투명할 뿐만 아니라 빅데이터 분석이 다양한 인과관계를 위장할 가능성을 높인다.[130]

2) 「유럽연합 인공지능법」의 리스크 관리와 기본권 보장

가) 「인공지능법」에 따른 인공지능 리스크 관리와 기본권 보장

인공지능 규제의 논의가 개인정보보호의 차원에서 알고리즘에 의한 인공지능의 '자동화된 의사결정'이나 '자동화된 처리'를 중심으로 논의되고 있으나, 인공지능기술의 발전 속도와 변화의 폭을 생각할 때 그것이 우리의 삶을 어떻게 변화시킬 것인지 전망하기는

---

125) 한편, 김희정, 위의 논문, 227-228면은 인간의 개입권은 정보 자체를 보호하거나 통제하는 것이 아니라 자동화된 의사결정의 영향으로부터 개인을 보호하기 위해 알고리즘 결정의 검증가능성과 정정가능성을 제공하는 것이라는 점에서 엄밀히 '개인정보'의 '보호'권에 해당한다고 분류하기 어려운 면이 있으나 그러한 측면이야말로 개인정보자기결정권이 갖는 인격권의 성격을 드러내는 것이라고 하고 있다.

126) 오정하·김일환, 지능정보사회에서 알고리즘의 법·규제의 방향, 법과 정책 제27권 제3호, 2021. 12. 119면.

127) 정종섭, 헌법학원론 723면.

128) 문의빈, 알고리즘 기반 추천과 플랫폼의 기본권 제한에 관한 비교법적 연구, 헌법학연구 제29권 제2호, 2023. 6. 411면.

129) 문의빈, 플랫폼 뉴스 서비스와 알 권리, 언론과 법 제22권 제1호, 2023, 218-222면. 기타 관련 문헌으로 권은정, 지능형 미디어 영역의 알 권리에 관한 공법적 고찰, 법학논총 제38집 제1호, 2021; 김희정, 위의 논문(2020); 박상돈, 헌법상 자동의사결정 알고리즘 설명요구권에 관한 개괄적 고찰, 헌법학연구 제23권 제3호, 2017 등을 참조.

130) Trute, 김태호 역, 빅데이터와 알고리즘 : 독일 관점에서의 예비적 고찰, 경제규제와 법 제8권 제1호, 2015. 5. 98면.

매우 어렵다. 특히 데이터를 분석하고 예측하는 데 주력하는 기존 AI에서 스스로 학습하고 데이터를 생성하는 생성형 인공지능(Generative AI)을 넘어 언제 범용인공지능 또는 일반인공지능(Artificial General Intelligence, AGI)에 도달할 것인지 그 예상시점은 점점 단축되는 것으로 보인다.

2024. 3. 13. 유럽연합 의회를 통과하여 최종 법률안을 성안중인 「유럽연합 인공지능법」(Artificial Intelligent Act, '인공지능법'이라 한다)[131]은 인공지능의 사용례에 따라 발생할 수 있는 위험을 등급화하여 대처하는 방식을 택하고 있다. ① 사람의 의식 이면 잠재의식을 이용하거나 사람의 의사결정 능력을 손상시키는 시스템, ② 사람이나 특정 단체의 취약성 활용하는 시스템, ③ 특정 사람 또는 단체에 대해 불공정한 처우를 하거나 사회적 점수를 매기는 평가 또는 분류 목적의 시스템, ④ 실시간으로 원격 생체인식 식별시스템을 이용 하는 인공지능활동은 금지된다(제5조).

또한 건강, 안전, 기본권에 중대한 위해를 끼칠 위험이 있는 인공지능 시스템은 '고위험'(high-risk) 인공지능으로 분류(제6조 제2항)하여 리스크 관리시스템을 구축하고 투명성의무를 비롯한 다양한 의무를 부과(제9조 이하)하고 있다. 인공지능 시스템에 대해서는 투명성 의무(제52조 제1항~제3항)을 두어 사람과 교류하는 인공지능 시스템은 그 제공자, 사용자, 해당 인공지능 시스템으로 하여금 사람이 AI 시스템과 교류하고 있음을 적시에, 명확히 고지해야 하고, '진정하거나 진실한 것으로 오도되는 텍스트, 오디오 또는 시각적 콘텐츠와 동의없이 그 사람이 실제로 하지 않은 말 또는 행동을 묘사하는 것'으로 정의되는 이른바 '딥페이크'의 경우에도 이에 관한 내용을 분명하게 시각적 방법으로 콘텐츠에 표시하도록 하고 있다.

또한 생성형 인공지능에 대해서도 그에 대한 고지의무와 특히 표현의 자유를 포함한 기본권을 침해해서는 안 된다고 하고, 유럽연합 또는 회원국의 저작권 보호, 저작권법 보호대상인 훈련 데이터 사용시 주요 내용의 공개 의무를 정하고 있다(제28조 제b항).

나) 인공지능기술의 가능성과 기본권 보장의 안전장치

「인공지능법」의 리스크 규율은 인공지능의 비약적인 발달이 가져올 사회적 위험성을

131) 현재시점의 법안은, Gesetz über künstliche Intelligenz. Legislative Entschließung des Europäischen Parlaments vom 13. März 2024 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, P9_TA(2024)0138 참조.

사전에 예방하려는 취지를 담고 있다. 인공지능에 대한 우려는 앞서 본 디지털 전환에 따른 개인정보자기결정권의 강화된 보호 필요성을 넘어서는 요소를 안고 있는 것으로 보인다.[132] 이는 단기적으로는 인공지능의 부정확성으로 인한 리스크(환각, 부정확한 예측)에서부터 기술적 고도화로 인해 인간의 인지능력에 대한 한계를 넘어서는 조작(가짜뉴스, 딥페이크 등)이나 왜곡(필터버블, 차별), 고도의 통제시스템이 구축(생체정보 활용 등을 통한 감시)되는 것에 대한 우려이지만, 다른 한편으로는 인간의 존엄성에 대한 본질적 제약이 초래될 수 있다는 우려의 측면 또한 갖고 있다(기계에 의한 지배나 기계에 대한 과도한 의존[133]). 인공지능에 의한 의사결정이 판단자로 하여금 무사유의 상태로 만들어 자동화편향에 의존하도록 한다거나, 시스템의 결과에 종속되지 않고 추가적인 최종판단권을 부여하는 경우에도 사후적 책임을 두려워하여 이를 그대로 따를 가능성이 있다는 지적도 같은 맥락이다.[134] 앞서 자동화된 의사결정에서 살펴본 바와 같이 이러한 의사결정과정에서 대상자에 대한 탈인격화가 일어날 위험이 상존한다.

이러한 우려가 어느 정도 현실화할 것인지는 지켜봐야 할 것이지만 불확실한 기술 발전의 전망 속에서 사회적 위험을 조율하기 위해서 헌법적 위상을 갖는 규제의 일반적 원칙을 (적어도 윤리적 차원에서부터) 형성해 두는 것이 필요한 것은 분명하다. 이를 위해 유럽연합 인공지능법 등에서 제시되고 있는 투명성과 설명책임성 원칙을 좀 더 살펴보기로 한다.

다) 인공지능의 설명책임성과 투명성 요청

인공지능에 대해 요구되는 설명책임성은 이미 GDPR에서 논의된 '설명을 요구할 권리'를 적용하는 방식으로 이루어질 수 있다.[135] GDPR이 설명을 요구할 권리를 명문화하고 있지는 않지만, 개인정보처리에 대해 적법성과 공정성, 투명성을 요구하는 조항으로부

132) 특히 인공지능 위험에 대해서는 위험인지에서 다양한 층위가 있음이 지적된다. 최은창, 인공지능 위험인지의 차이와 거버넌스, 한국인공지능법학회, 인공지능 윤리와 거버넌스, 2021, 146면 이하를 참조.

133) 인공지능에 대한 무엇을 하는지 모르면서 점점 더 의존하게 되고, 의존도가 커지면서 부당한 영향에 대한 취약성이 발생하여 '인지적 자유에 대한 제약'이 초래된다는 지적이 있다. Farahany, N. A. (2023), The battle for your brain: defending the right to think freely in the age of neurotechnology, St. Martin's Press. 정인영, 생성형 인공지능 발전과 공법의 역할: 미국 법제도를 중심으로, 정보통신정책학회 학술대회 자료집(2023. 11. 17. 170면)에서 재인용.

134) 박원규, 인공지능, 빅데이터, 그리고 경찰, 공법학연구 제24권 제1호, 2022, 342면.

135) 관련 논의로, 이희옥, 인공지능 의사결정에서의 이익조정과 이원적 규제모델에 관한 연구, 행정법연구 제63호, 2020. 10. 281면 이하를 참조.

터 설명책임성을 도출해 볼 수 있다는 것이다. 설명요구권에 대해서는 알 권리로부터 도출된다고 하기도 하고, 개인정보자기결정권의 일종으로 설명되기도 한다.[136] 설명요구권은 사후적으로 문제가 발생했을 때 알고리즘에 대한 입증의 부담을 전환하는 기능을 한다고 하기도 한다.[137]

문제는 생성형 인공지능과 같이 스스로 학습하는 알고리즘의 경우 등에서 실제 설명을 요구할 권리가 어느 정도 현실화될 수 있을 것인가이다. 생성형 AI의 알고리즘이 과연 블랙박스와 같은 것이라면, 정보주체가 사전에 정보에 대한 수정의 기회를 갖기 어려운 것은 물론이고 인공지능이 스스로 추가 생산한 판단에 대해 개입하는 것이 현실적으로 어려울 가능성이 크기 때문이다.[138] 이 점에서 "데이터의 수집 방식, 목적, 사용의도, 알고리즘의 작동방식, 모델링 프로세스나 데이터의 가중치"[139]에 대해 어느 정도 설명하여야 설명책임성을 다하는 것인지에 대해 향후 논의를 지속해 나가야 할 것이다.[140] 기실 인공지능의 의사결정과 관련하여 언제나 인간이 이해할 수 있도록 설명이 필요한 것은 아니며 설명가능성이 필요한지, 설명이 유용한지는 인공지능을 둘러싼 다양한 관계 속에서 설명이 되어야 하는 문제이다.[141] 또한 인공지능 맥락에서의 '설명가능성'이 제대로 작동하려면 설명가능성을 평가할 수 있는 기준과 인공지능의 신뢰성, 투명성, 책무성을 관리하는 절차와 수단이 개발되어야 한다고 한다.[142] 투명성은 제3자 또는 감독기관이 시스템을 평가하거나 접근할 수 있도록 하는 절차를 통해 구현될 수 있기 때문이다. 최근에는 설명가능한 알고리즘에 대해 인공지능의 행위와 판단을 사람이 이해할 수 있는 형태로 설명할 수 있는 설명가능한 인공지능(Explainable AI, XAI)을 통한 해법이 모색되기도 한다.

---

136) 오정하·김일환, 지능정보사회에서 알고리즘의 법·규제의 방향, 법과 정책 제27권 제3호, 2021, 121면 이하.

137) 가령 오정하·김일환, 위의 논문, 118면 이하, 128면.

138) 이형석·전정환, 빅데이터를 기반으로 한 인공지능 예측력의 헌법적 쟁점에 관한 연구, 원광대학교 법학논총 제29집 제1호, 2021. 4. 42면.

139) 황용석·김기태, 알고리듬 기반 자동화된 의사결정의 설명 가능성에 대한 연구, 언론정보연구 제57권 제3호, 2020, 53면 참조.

140) 최근의 연구로, 이대희, 인공지능에 의한 개인정보의 자동 처리에 대한 투명성 확보에 관한 연구 – 알고리즘에 의한 자동 의사결정에 따른 '설명요구권'을 중심으로, 저스티스 200호, 2024. 2. 참조.

141) 고학수·박도현 외, 인공지능원론, 13면.

142) 김법연, 인공지능 통제수단으로서 주요국 규제 입법의 동향과 시사점, 유럽헌법연구 제42호, 2023. 8. 281-283면.

나. 유럽연합 디지털 권리선언과 디지털 전환의 사회적 권리

1) 유럽연합 디지털 권리선언의 개요

유럽연합의 경우 스페인·포르투갈 등의 디지털 기본권 선언을 수용하여 EU 디지털 권리선언을 내놓기도 하였다. 유럽연합 집행위원회는 2030년까지 디지털 전환에 관한 방향과 목표를 담은 '2030 디지털 전환의 나침반(2030 Digital Compass: the European way for the Digital Decade, 2021. 3. 9.)을 제시한 바 있고,[143] 이후 이를 반영하여 디지털화에서의 규범적 원칙과 권리에 관한 '디지털 권리와 원칙에 관한 유럽 선언'(European Declaration on Digital Rights and Principles, 이하 '**EU 디지털 권리선언**')[144]을 공표하였다. 이 선언은 디지털 전환 과정에서 요구되는 다양한 권리의 맥락과 방향성을 드러내는 의미가 있는 것이었다. 이와 같은 논의가 선언의 형태로 이루어진 것은 지능정보기술 발달의 가변성과 불명확성을 고려하여 디지털 전환의 전개에 대해 바로 어떤 규율을 하기보다는 법적 구속력이 없이 사회적 합의를 형성해 가는 시도라 평가할 수 있다. 이 논의는 입법과 행정에 대한 가이드라인으로서의 기능을 수행함으로써 미래의 법발전에 대한 방향성을 가늠할 수 있게 한다. 이 선언은 실제 디지털 투명성 강화에 대한 「인공지능법」이나 「디지털 서비스법」, 온라인 안전 및 보안에 관한 GDPR, 디지털 참여 가능성의 확대(「디지털 서비스법」 등)로 구현 과정에 있다.

유럽연합의 디지털 권리 선언은 디지털 전환에서 주요한 원칙과 권리를 제시하면서, 이를 인간 중심의 전환, 연대와 포용, 선택의 자유, 디지털 공공 공간 참여, 안전 보안의 권한, 지속가능성을 핵심 항목으로 제시하면서 24개 사항을 선언의 형식으로 발표하였다. 이하에서는 그 중에서 아직 충분히 구현되고 있지 않은 디지털 접근권과 디지털 격차해소권에 관한 기술을 살펴보기로 한다.

2) 디지털 접근권의 강화 선언

디지털 권리선언은 사회국가적 생존배려의 관점에서 최소한의 네트워크, 기기, 데이터

143) https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (2024. 2. 29. 최종방문) 참조

144) EU는 2022. 1. 선언문 초안을 발표하고, 유럽의회, EU 이사회, EU 집행위원회가 공동서명하여 2022. 12. 15. 최종 선언문을 채택하였다. https://digital-strategy.ec.europa.eu/en/policies/digital-principles 참조

를 이용할 수 있는 권리를 보장해야 한다고 선언하고 있다. 이는 인터넷 네트워크에 접속할 수 있는 권리뿐만 아니라 접속을 위해 필요한 전자기기의 이용권, 필요한 최소한의 데이터를 사용할 권리를 포함할 수 있어야 한다는 선언이다. 즉 EU 디지털 권리선언 제3조는 인터넷 네트워크 및 기기 접근권, 플랫폼 이용권, 데이터 이용권을 포함한 디지털 접근권을 서술하고 있다. 이러한 디지털 접근권은 일반적 행동 자유를 위한 전제적 기본권이며 적극적인 보장을 요구하는 사회적 기본권에 대한 요청으로 이해된다. 종래 디지털 접근권은 인터넷에 대한 접근성 보장을 중심으로 논의되어 왔는데, 이는 네트워크 뿐만 아니라 소프트웨어나 기기를 포괄하는 의미를 가질 수 있다.[145] 여기서 '접근권'의 의미는 모든 국민이 향유하는 자유라는 차원에서의 '접근권', 정보주체의 자신의 정보에 대한 '접근권', 사회적 약자가 디지털을 이용하는 데 있어서 동등한 접근의 조건이 부여되어야 한다는 의미에서의 '접근권'이 모두 담길 수 있다.[146] 다만, 후자는 이하에서 보게 될 디지털 격차해소권의 차원에서 접근할 수도 있을 것이다.

> (EU 디지털 권리 원칙) 3. EU 전역의 모든 사람은 저렴하게 고품질 디지털에 접속할 수 있어야 한다.
>
> a. 저소득층을 포함한 EU의 모든 사람이 인터넷에 접근할 수 있는 고품질 연결에 대한 접근(access)를 보장한다.
>
> b. 콘텐츠, 서비스 및 애플리케이션이 부당하게 차단되거나 저하되지 않는 중립적이고 개방적인 인터넷을 보호하고 촉진한다.

이상의 규정은 유럽연합 디지털 권리선언을 참고한 한국의 '디지털 권리장전'에서도 유사한 규정을 발견할 수 있다.[147] 공공서비스 차원에서의 디지털 접근권을 선언한 유럽연합의 다음 규정도 한국의 디지털 권리장전에서 찾을 수 있다.[148]

> (EU 디지털 권리 원칙) 7. 누구나 EU의 주요 공공 서비스에 온라인으로 접근할 수 있어야 한다. 누구에게도 디지털 공공 서비스에 접근하고 사용할 때 필요 이상으로 더 자주

145) 가령 김민호, 인터넷접근성 보장 및 국가의 역할, 성균관법학 제27권 제3호, 2015. 9, 4면 이하 참조.
146) 김민호, 위의논문, 6면.
147) (디지털 권리장전) 제6조 디지털 접근의 보장. 모든 국민은 일정한 품질을 갖춘 안정적인 네트워크 환경을 보장받아야 하며, 이를 바탕으로 다양한 디지털 서비스에 언제 어디서나 차별없이 접근하여 이용할 수 있어야 한다.
148) (디지털 권리장전) 제15조 데이터의 개방은 촉진되어야 하며, 특히 공공데이터는 접근과 이용의 기회가 공정하게 보장되고 그 이용권의 보편적 확대를 위해 필요한 조치가 이루어져야 한다.

데이터를 제공하라는 요청을 받아서는 안 된다.

a. EU에 거주하는 사람들에게 광범위한 온라인 서비스에 대한 접근을 제공하는 접근 가능하고 자발적이며 안전하고 신뢰할 수 있는 디지털 신원을 사용할 수 있는 가능성을 보장한다.
b. 공공 부문 정보의 광범위한 접근성 및 재사용을 보장한다.
c. 특히 디지털 건강 및 의료 서비스, 특히 전자 건강 기록에 대한 접근을 포함하여 효과적인 방식으로 사람들의 요구를 충족하도록 설계된 디지털 공공 서비스에 대한 EU 전역의 원활하고 안전하며 상호 운용 가능한 접근을 촉진하고 지원한다.

3) 디지털 격차해소권의 선언

정보사회에서의 디지털 격차(digital divide)는 디지털 전환 과정에서 가속될 수 있다. 디지털 사회에서 디지털 격차에 따른 디지털 소외는 기본권 행사 자체를 곤란하게 할 수 있다. 디지털 소외계층이 디지털 사회에서 자유를 향유할 수 있도록 실질적 조건을 마련하는 것은 지능정보사회에서 핵심적인 사회국가의 과제이다.[149]

인터넷 네트워크와 서비스에 접근할 수 있는 권리는 빈곤층, 장애인, 고령자와 같은 디지털 소외계층이 실질적으로 해당 서비스를 이용하기 용이하도록 이용 비용과 서비스가 설계되어야 한다는 측면의 권리와 이러한 네트워크와 서비스를 실질적으로 이용할 수 있도록 하는 역량을 갖거나 지원을 받을 수 있는 권리라고 할 수 있다.[150]

(EU 디지털 권리 원칙) 2. 기술은 사람을 분열시키는 것이 아니라 통합하는 데 사용되어야 한다. 디지털 전환은 EU의 공정하고 포용적인 사회와 경제에 기여해야 한다.

a. 기술적 해결책의 설계, 개발, 배치 및 사용이 기본권을 존중하고, 기본권을 행사할 수 있게 하며, 연대와 포용을 촉진한다.
b. 모두가 뒤처지지 않는 디지털 전환. 이는 모든 사람에게 혜택을 주고, 성별 균형을 달성해야 하며, 특히 노인, 농촌 지역에 거주하는 사람, 장애인, 소외된 사람, 취약하거나 권리를 박탈당한 사람들을 포함해야 한다. 또한 문화적, 언어적 다양성을 촉진해야 한다.
c. 디지털 전환의 혜택을 받는 모든 시장 행위자가 EU에 거주하는 모든 사람들의 이

149) 성관정, 디지털 격차 해소를 위한 인터넷 접근권에 관한 연구: 사회적 기본권을 중심으로, 서울대학교 박사학위논문 2022. 8. 또한 같은 취지이다.

150) (디지털 권리장전) 제15조 (디지털 리터러시 향상) 디지털 기술의 개발과 사용의 기회를 보장할 수 있도록 디지털 격차가 해소되어야 하고, 디지털 리터러시 향상을 위한 교육의 기회가 제공되어야 한다.

익을 위해 사회적 책임을 맡고 공공재, 서비스 및 인프라 비용에 공정하고 비례적으로 기여할 수 있도록 적절한 체계를 개발한다.

4. 모든 사람은 교육, 훈련 및 평생 학습에 대한 권리가 있으며 모든 기본 및 고급 디지털 기술을 습득할 수 있어야 한다.
   a. 디지털 성별 격차를 해소하기 위한 견해를 포함하여 고품질 디지털 교육 및 훈련을 촉진한다.
   b. 모든 학습자와 교사가 미디어 문해력, 비판적 사고를 포함하여 필요한 디지털 기술과 역량을 습득하고 공유하여 경제, 사회 및 민주적 과정에 적극적으로 참여할 수 있도록 지원하는 노력.
   c. 모든 교육 및 훈련 기관에 디지털 연결, 인프라 및 도구를 갖추기 위한 노력을 촉진하고 지원한다.
   d. 기술 향상 및 기술 재교육을 통해 작업의 디지털화로 인한 변화에 모든 사람이 적응할 수 있는 기회를 제공한다.

Ⅲ. 디지털 전환 시대의 기본권 보장 방식·체계와 국가임무

1. 디지털 전환의 변화하는 사회상

가. 디지털 전환을 가속화하는 디지털 기술과 사회 변화

1) 디지털 전환의 문제 국면들

Ⅱ.장에서 유럽연합과 독일의 사례를 중심으로 디지털 전환의 여러 국면을 살펴보았는데, 여러나라가 공유하는 디지털 전환의 문제상황을 다시 한번 정리하면 다음과 같다.

한국에서도 디지털화의 순기능과 역기능에 대한 사회적 문제의식은 이미 학교별학교종합정보관리시스템을 온라인으로 연계·관리하는 교육행정정보시스템(NEIS)을 도입하기로 한 2000. 9. 정책에 대한 헌법소원에서 시스템 도입이 개인정보자기결정권을 침해한다고 본 반대의견에서 일찍부터 피력된 바 있다.[151]

> 수기가 아니라 컴퓨터파일의 형태로 개인정보를 보유·처리할수록, 분산 보유하는 경우보다 하나의 통합체계로 개인정보를 관리할수록, 개인정보의 접근·결합·이용이 용이하게 되므로 강화된 보호가 필요하다. 그 자체로는 보호의 필요성이 크지 않은 산발적 개인정보일지라도 컴퓨터에 의한 정보처리의 경우 자동검색체계를 통하여 다른 개인정보들과 유기적으로 결합함으로써 개인의 전체적·부분적 인격상이 국가권력의 감시·통제와 지배 하에 놓일 수 있다."

물론 당시 전자정부 사업의 일환으로 명확한 법률적 근거 없이 시작된 이 사업에서 최초 학부모의 직업과 최종학력 등까지 모두 기입하도록 되어 있었다는 무신경을 보면 지금 시점에서 볼 때 당시 개인정보보호에 대한 일반적인 문제의식이 지금과 유사하다고 할 수는 없을 것이다. 졸업생의 성명, 생년월일, 졸업일자를 수록한 것을 심판대상으로 삼은 헌법소원에 대해 당시의 다수의견은 "교육부 등이 보유목적을 벗어나 개인정보를 무단 사용했다는 점을 인정할 자료가 없는 한 NEIS라는 자동화된 전산시스템으로 그 정보를 보유하고 있다는 점만으로 적법한 보유행위 자체의 정당성마저 부인하기는 어렵

151) 헌재 2005. 7. 21. 2003헌마282등, 판례집 17-2, 81, 96의 반대의견.

다”[152]고 판단하였다.[153] 이렇게 정보가 집적된 NEIS에는 이후 재학생·졸업생의 신상·성적·건강정보가 포함되게 되었고, 현재는 차세대 교육행정정보시스템으로 변화되기에 이르렀으며, 차세대 교육행정정보시스템 사업을 통해 빅데이터, 인공지능, 지능형 클라우드 기술이 도입된다고 알려지고 있다.[154] 디지털전환의 일부라 할 NEIS 사업은 오늘날, 그리고 미래에 어떤 헌법적 평가가 가능할 것인가.

디지털화가 정보의 규모와 집중에 의해 확대되는 현상은 이제 새로운 문제 양상으로 변모하고 있다. 디지털화가 전자화된 정보를 사용하여 기존의 작업 방식을 더 간단하고 효율적으로 만드는 현상이라고 한다면, 막대한 디지털 정보의 생산과 그 활용 가능성은 새로운 형태의 경제적 활동과 서비스 창출의 동력이 되고 있다. 디지털 데이터는 복제가 용이한 속성을 갖고 복제된 데이터가 원본과 동일하며 영구적 보존이 가능하고 표준화된 정보처리를 가능하게 하는 특징이 있다는 점[155]은 광범위한 활용의 원동력이 되었다.

이처럼 디지털 전환이 자유의 관점에서 볼 때 자유의 확대와 제한을 동시에 광범위하게 일으키는 효과를 낳기 때문에 지능정보기술의 발달과 데이터의 경제적 활용 가치 증대에 따른 디지털 전환은 다음과 같은 상황에서 디지털 전환에 대한 편익과 불이익을 균형있게 고려해야 하는 상황을 맞게 되었다.[156]

첫째, 디지털 전환은 초연결사회를 낳는다. 사람과 사람, 사람과 사물이 연결되도록 하는 기술적 발전은 사람과 주변의 세계가 상호작용하는 방식을 새로운 국면으로 인도했는데, 이러한 과정에서 개인정보가 수집되고 활용되는 규모와 방식에 질적인 변화가 일어났다.

둘째, 이처럼 데이터가 갖고 있는 경제적 가치와 혁신에서의 중요성이 폭발적으로 증가한다. 데이터 경제는 데이터의 유통으로 제반 산업 발전의 촉매가 되고 새로운 서비스를 창출하는 경제 활동을 가리키는 것인데, 이로부터 창출된 혁신적인 서비스는 사회 전

152) 헌재 2005. 7. 21. 2003헌마282등, 판례집 17-2, 81.

153) 다만, 이 결정에서 재판관 1인은 학력에 관한 정보가 민감한 정보로 취급되는 우리 사회에서 “개인정보보호법제도 완비되지 않은 상황에서 결코 가벼이 취급할 수 없는 개인정보를 피청구인들이 NEIS에 보유하고 있는 행위는 개인정보자기결정권을 침해하는 것”이라는 반대의견을 내기도 하였다.

154) 그러나 최근 개통된 4세대 NEIS는 오류를일으켜 접속불량, 시험답안 유출의 보안 사고가 발생하여 사회적 문제가 되었다. 경향신문, 2800억 들인 차세대 나이스 개통 3주째···교사 10명 중 8명 “여전히 불편”, 2023. 7. 13. 기사 참조.

155) 황성기, 디지털 기본권의 의미와 내용, 헌법학연구 제24권 제3호, 2018, 8면.

156) 이인호, 지능정보사회에서 개인정보보호의 법과 정책의 패러다임 전환, 2022. 같은 취지로, 이권일, 지능정보사회에서 개인정보자기결정권이 보호하고자 하는 헌법적 가치, 공법연구 제51집 제3호, 2023. 2.; 정애령, 지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호, 공법학연구 제23권 제1호 참조.

체적 가치를 증진시키는 의미를 가진다.

셋째, 데이터의 활용 가능성이 커지면서 서비스의 질을 제고하기 위한 개인정보의 가치가 매우 중요해졌다. 이로 인해 개인정보는 인격의 일부이면서 일종의 재화로서 경제적 가치가 부여되게 되었다(commondification of personal data). 그 결과 개인이 자신을 드러내고 연출함으로써 경제적 가치를 획득할 수 있다는 사실이 개인정보의 가치에 대한 보호에 무관심하게 되는 역설(privacy paradox)을 초래함으로써 개인정보의 남용을 허용할 가능성이 더 커지게 되었다.

넷째, 인공지능의 발달은 다시 한번 데이터를 활용한 서비스의 비약적인 성장을 가져왔으나 다른 측면에서 개인정보보호체계의 근본적 한계를 노정하게 하였다. 빅데이터를 통해 인공지능이 학습하여 결과를 도출하는 방식은 방대한 데이터에서 상관관계(correlation)를 찾도록 하는 알고리즘에 따른 것인데 그러한 알고리즘을 통해 어떤 결과가 나올 것인지에 대해서 예측이 불가능하고 오늘날 이른바 방대한 신경망을 통해 얻은 정보를 통해 이른바 심층학습(deep learning)을 하는 인공지능의 처리 결과를 설계자도 설명하기가 어렵게 되었다(black-box effect).

2) 디지털 심화의 문제 국면들

디지털 전환 과정은 이제 디지털 기술과 활용이 국가사회의 운영과 개인 활동 전반에 내면화하는 과정을 거치고 있다. 이는 특히 인공지능이 발전하면서 디지털 정보를 활용하고 응용할 수 있는 기술적 발전이 급속히 이루어진 데 따른 것으로, 특히 생성형(Generative) 인공지능 기술이 범용기술로서 발전해 나가는 과정 속에서 패러다임 전환적 변화를 맞고 있다. 이제 인공지능이 인간만의 영역으로 간주되었던 창작의 영역에서까지 인간을 능가하는 기술을 보여주고 있다. 생성형 인공지능은 대규모 데이터세트를 기반으로 훈련된 딥러닝(deep learning)[157] 모델을 사용하여 스스로 새로운 콘텐츠를 생성하는 인공지능 모델을 가리킨다. 생성형 인공지능은 미래에 일반인공지능으로 발전하는 것을 목표로 한다.

이러한 디지털 심화 단계에서 출현하는 강력한 형태의 인공지능에 대한 기대와 우려

157) 대량의 데이터를 분석하고 해석하기 위해 컴퓨터가 인간이 지식을 얻는 방식을 모방하여 관찰을 통해 학습하도록 가르친다. 딥러닝은 인간 언어를 컴퓨터에 이해시키는 기술, 즉 이른바 자연어 처리(NLP)에서 중요하다.

는 기술발전이 초래하는 디스토피아와 관련하여 예측할 수 없는 위험에 대한 사전 방지의 필요성을 강화한다. 여기서 통제할 수 없는 거대규모의 인공지능기술에 대한 알 권리와 기술통제의 문제가 기본권적 차원에서 더 주목받기 시작하게 된 것이다. 한편으로 이 단계에서는 데이터 활용의 고도화에 따라 인공지능의 사용으로 사생활의 보호가 사실상 무의미해질 가능성에 대해서도 좀 더 시스템 차원에서의 접근을 요구받게 된다.

반면 인공지능이 가져온 영향력이 사회적인 위험으로 발전할 가능성에 대한 경계도 더욱 커지게 되었다. 생성형 인공지능으로 인한 데이터편향, 허위정보, 정보왜곡 등 개인정보보호를 넘어선 인공지능이 학습 데이터의 문제 등 새로운 문제가 부각되게 되었다.[158]

나. 디지털 전환에 따른 사회 영역별 변화

1) 디지털 행정

행정을 중심으로 한 공적 영역에서의 디지털 전환 활동은 전자정부(E-goverment)의 구축과 전자적 행정작용을 통해 구체화된다. 디지털 전자정부를 통한 기술 발전과 전자행정은 행정 접근성을 높여줄 수 있지만 역설적이게도 정보통신기술을 이용하기 어려운 사람에게 정보활동 능력의 격차(Digital Divide)로 행정서비스의 접근가능성과 이용가능성을 떨어뜨리는 결과를 낳을 수 있다. 이는 오늘날 디지털 전자정부의 활성화(최근의 이른바 디지털플랫폼정부의 논의에서도)에서 중심적인 문제로서 비중있게 다루어져야 한다.

디지털 전환은 공적 영역과 사적 영역을 망라하여 우리 생활의 전 국면에서 진행된다. 공적 영역에서의 디지털 전환은 디지털 전자정부 플랫폼의 구축이나 입법·행정·사법 활동에서 디지털 기술의 활용을 통해 구체화된다. 공적 영역에서의 디지털 전환은 모든 시민이 그 전환에 접근하고 이용할 수 있는 기회를 보장하여야 한다는 점에서 사적 영역에서의 디지털 전환과 차이가 있다.

2) 디지털 경제

디지털 전환은 경제 영역에서 새로운 서비스와 재화를 창출하는 데 결정적인 기능을

158) 가령 김현진, 생성형 AI와 편향성, 인하대학교 IP & Data 법, 제3권 제1호, 2023. 6. 75면 이하 참조.

한다.[159] 디지털 경제가 갖는 특징은, 첫째, 디지털 경제를 통해 경제적 비용을 절감하고 효용을 높일 수 있다는 점이다. 검색비용, 복제비용, 배송비용, 추적비용, 검증비용 등이 절감되며 그 결과 디지털 경제주체는 경쟁에서의 우위를 점할 수 있다. 둘째, 디지털 경제가 구동하는 재화 및 서비스의 공급, 수요체계를 혁신하는 매개로서 온라인 플랫폼이 갖는 위상의 확대이다. 여기에는 플랫폼을 통한 정보의 집적 효과와 네트워크 효과가 갖는 의미가 크다. 셋째, 대규모 데이터의 집적, 유통, 생산 및 활용이 디지털 경제에서 차지하는 비중이 커지며, 데이터 자체가 갖는 경제적 가치가 강조된다. 이전에는 경제적 가치가 없던 파편화된 데이터가 기술발전으로 경제적 활용도가 생기면서 데이터의 중요성이 커지게 된다. 이처럼 플랫폼, 네트워크, 데이터는 디지털 경제를 이끌어가는 핵심 소재로서 오늘날 지능정보기술의 발달로 그 중요성이 더욱 커지게 된다.

디지털 경제와 같은 사적 영역에서의 디지털 전환은 디지털 경제에서 사기업 등에 의한 디지털 기술과 디지털 서비스를 고도화하는 형태로 이루어진다. 이 과정은 경제적 자유의 실현으로서 경제적 이윤동기에 의해 추동되므로, 시장경제에 대한 국가적 개입으로서 경제주체에 대한 기본권 제한의 정당화와 그 한계가 문제된다. 다만 디지털 경제에서는 예측가능한 사전의 규칙을 정하거나(가상자산에 대한 규율) 인프라 이용에 대한 규칙을 정하는 (망중립성 원칙에 대한 규율) 국가의 기능 역시 간과되어서는 안 된다.

디지털 경제 영역에서는 온라인 플랫폼을 거쳐야 경제활동 및 일상활동이 가능하게 되는 경우가 많은데, 이는 디지털 전환 과정에서 디지털 정보가 유통되는 마당으로서의 플랫폼이 정보집적 등으로 인해 시장에서 독과점적 지위를 갖게 되는 경우가 흔하다. 오늘날 전세계적으로 이른바 빅테크(Big Tech)기업이라 불리는 초거대기업(대표적으로 GAFA─구글, 애플, 페이스북, 아마존─와 마이크로소프트)은 모두 인터넷 네트워크를 이용한 경제활동의 문지기(Gatekeeper)로서 플랫폼기업들이며 디지털 전환에 따른 데이터 및 정보의 독점으로 막대한 부를 누리고 데이터를 활용하는 기술발전에서 유리한 위치를 선점하고 있다. 디지털 정보를 집적할 수 있는 지위에 있는 플랫폼 기업은 인공지능 기술 개발에 대단히 중요한 양질의 정보를 보유하여 이를 자신의 경제적 서비스와 결합할 수 있는 기회를 갖게 되는 것이다.

이처럼 디지털 전환 과정에서 지능정보기술과 데이터 집적을 통해 양질의 서비스를

159) 이하의 요약은, 이원우·김태호, 디지털 경제 전환에 대응하는 경제규제체계의 전환, 2021. 12. 4면 이하를 참조.

제공하는 온라인 플랫폼 기업에 대해서는 경제적 주체 간의 우열관계(갑을관계), 소비자 보호, 독과점 강화 방지에 대한 국가적 개입의 필요성이 있는데, 이는 한편으로 경제적 주체인 온라인 플랫폼 기업의 경제적 자유에 대한 제한의 문제이자 온라인 플랫폼 기업에 대한 개입을 통한 국민의 기본권 보호의무 이행의 문제이다.

3) 디지털 커뮤니케이션

디지털 전환은 컴퓨터나 모바일 기기 등을 통해 문자, 이미지, 영상, 음성 등 전자적 전송물을 교환하게 하는데, 이러한 활동은 디지털 공간에서 다양한 형태의 표현물을 양산하는 표현행위이기도 하다. 디지털 전환을 통해 사람들은 다양한 형태로 많은 정보를 향유할 수 있게 있게 되어 더 많은 인격발현의 기회를 가질 여지를 가진다. 정치적 의사표현에 있어서 특히 디지털 기술을 활용한 전자민주주의의 가능성 확대는 공간적·시간적 한계를 넘어서는 정치적 자유의 확대 가능성을 가져 온다.

디지털 권리장전은 디지털 표현의 자유에 대해 규정하면서, 모든 국민은 디지털 환경에서 자신의 사상이나 의견을 원하는 방식으로 자유롭게 표명할 권리를 가진다고 하고 있다. 문제는 특히 사이버 공간에서 디지털 표현의 자유로서 익명 표현의 자유가 논의되기는 하는데, 이는 디지털 환경에서 익명, 가명 표현의 방식까지 표현자가 스스로 정할 수 있는가의 문제가 제기된다. 익명 표현의 자유는 인터넷에서의 표현의 자유 행사의 핵심 내용이며, 인터넷 표현의 자유에 대한 제한은 인터넷의 민주주의적 가치를 훼손하지 않도록 하는 데 유의해야 한다.[160]

디지털 전환은 직접적으로 의사표현의 자유나 알 권리를 진작하여 디지털 커뮤니케이션을 확대하는 효과를 가져올 수 있다. 이러한 활동은 많은 경우 포털 서비스나 소셜 미디어, 메시지 전송 플랫폼 등의 인터넷 플랫폼을 통해 이루어진다. 이로 인해 디지털 전환에서 인터넷 플랫폼은 이른바 OTT(Over the Top) 서비스로서 전통적인 언론 영역에서의 언론의 자유·방송의 자유가 논의되는 뉴미디어로서의 언론 주체 기능을 수행하기도 한다.

반면 디지털 커뮤니케이션의 증대는 다양한 이해관계의 충돌을 낳을 수 있다. 이해관계의 충돌을 통해 드러나는 기본권 충돌의 문제는 디지털 전환이 가져오는 공익적 가치

160) 장선미·성기용, 익명표현의 자유에 대한 헌법적 검토, 이화여대 법학논집 제20권 제4호, 2016. 6. 181면; 이부하, 위의 글, 145면.

와 다양한 기본권적 이익 간의 충돌이기도 하다. 디지털 사회의 의사소통 영역에서 온라인 플랫폼 기업의 상당수는 디지털 경제기업이면서 동시에 의사소통의 매개기업으로서의 핵심적인 지위를 가진다. 오늘날 주요한 소셜미디어(SNS)는 전통적인 언론의 기능을 대체하고 있으며, 이러한 정보를 매개하고 중개하는 사업자(intermediary)로서 정보유통의 장을 제공한다. 디지털 정보 유통의 특성이라 할 쌍방향의 의사소통을 통해 사회적으로 개인의 의사를 저비용으로 확산할 수 있도록 하는 민주적 공론의 소통장을 제공하는 것이다. 그러나 다른 한편 플랫폼 사업자는 가짜뉴스(fake news)에 대한 유통책임에서 드러나는 바와 같이 사적권력으로서 국가를 대신하여 스스로 디지털 감시를 수행해야 하는 이중적 지위를 가진다.

2. 디지털 전환에서 디지털 기본권의 보장

가. 디지털 전환이 기본권에 미치는 이중적 성격

이상에서 살펴본 바와 같이 디지털 전환이 가진 여러 실제 국면은 다양한 방식으로 우리 삶에 영향을 미친다. 디지털 전환은 시간적·공간적 한계를 넘어서는 활동을 가능하게 함으로써 개인의 자유와 사회적 편익을 무한히 확장할 가능성을 갖는다. 코로나 19 사태로 촉발된 격리 상태에서 사회적 활동 수행을 가능하게 한 온라인 활동이나 생성형 인공지능을 활용한 정보 활용도의 증가 및 문제해결력의 강화가 단적인 예가 될 수 있다. 그럼에도 디지털 전환은 기술 발전이 초래할 수 있는 사회적 위험의 증가로 인해 종래에는 문제되지 않던 자유에 대한 위험이 현실화되거나 기본권 침해가 광범위하게 이루어질 가능성 또한 증대시킨다.

나. 디지털 전환의 특성을 반영한 체계적 검토의 필요성

1) 디지털 특성을 반영한 기본권 해석

이상의 논의를 보면 개인정보 자기결정권 등과 같은 디지털 시대의 기본권 뿐만 아니라 기본권이 보호범위를 확장함으로써 디지털 전환에서의 기본권 보장을 해석을 통해 해

결해야 하는 과제를 안고 있다는 점을 알 수 있다.[161] 가령 '사이버 집회', '사이버 주거'가 집회의 자유와 주거의 자유를 통한 보호를 받을 수 있는가와 같은 문제를 발생시킨다.

가령 사이버 집회가 헌법상 집회의 자유로부터 보호의 대상이 되는가는 이른바 분산 서비스거부(DDoS) 공격을 통해서 서버를 다운시키는 방식으로 사이버 공간에서 항의의 의사표시를 하는 것을 생각해 볼 수 있다. 이른바 특정 웹사이트에 접속자를 한꺼번에 몰아서 사회적 의사표시를 하는 이른바 플래쉬 몹(Flash-Mobs) 등 SNS에서 조직적 활동은 그것이 공공의 여론 형성에 영향을 미치는 것이라면 헌법적으로 보호될 수 있는 집회의 준비조치라고 볼 수 있다고 하기도 한다.[162]

다만 이러한 디지털 특성을 반영한 기본권 해석은 그것이 실정헌법의 가능한 문언 해석의 범위를 어느 정도까지 넘어설 수 있는지 해석의 한계에 관한 문제가 있을 수 있다. 독일의 경우 형체가 없는 가상 집회(virtuelle Versammlungen)에 대해 그것이 일반적 행동의 자유와 의사표현의 자유에 의해서는 보호되지만, 그것이 기본법 제8조에서 정한 집회에 해당하여 집회의 자유를 인정할 것인가에 대해서는 견해 대립이 있었다. 집회의 개념에는 다수의 사람들이 한 장소에서 동시에 지역적으로 회합(Zusammenkunkft)하고 형체를 갖고 참석한다는 것을 핵심 구성요소로 삼고 있다고 보았기 때문이다. 이것은 집회에서 사람들이 모여서 대화하고 내부 결속을 다지며 이를 외부적으로 표출하는 것이 개념적으로 중요한데, 방문자들의 홈페이지 접속으로 이러한 요건이 충족되었다고 할 수 있는지 의문이 제기되었다.[163] 이는 공간적으로 분리된 사람들이 다른 장소에서 작동한 전자 신호가 어떤 서버에서 함께 발견되는 현상에 해당할 뿐이고, 이를 집회로 포함되는 것으로 볼 수는 없다는 것이다. 그러나 이러한 이해는 아직 가상 집회라는 관념 자체가 존재하지 않던 시기의 법해석이므로 이를 그대로 적용할 수 없다는 반론도 가능하다.[164]

이러한 해석상의 쟁점은 '가상 주거'의 보호 등에서도 유사한 논의가 가능할 것인바 이는 디지털 전환의 특수성을 충분히 반영할 수 있는 방법으로 해석론을 전개할 필요도 있을 것이다.

---

161) 이러한 현상은 헌법변천과도 유사한 것이 될 수 있는데, 이에 대해서는 Peuker, Verfassungswandel durch Digitalisierung - Digitale Souveränität als Verfassungsrechtliches Leitbild, Tübingen 2020를 참조.

162) 조인성, 인터넷상 디지털 차원의 개별적 기본권에 관한 연구–독일에서의 논의를 중심으로, 홍익법학 제15권 제1호, 2014. 2. 14면에서 재인용.

163) BVerfGE 104, 92, 104. Hebeler/Berg, Die Grundrechte im Lichte der Digitalisierung–Teil III, JA 2021, 969, 973.

164) Pötters/Werkmeister, JURA 2013, 5, 9; Herbeler/Berg, 위의 논문, 973에서 재인용.

2) 헌법상 권리와 법률상 권리의 구분 필요성

디지털 권리는 헌법적 차원의 권리일 수도 있고 법률적 차원의 권리일 수도 있다. 자유권적 성격의 디지털 권리는 법률에 의해 그 내용이 규정되어 있다고 하더라도 사실상 헌법상 권리의 확인적 성격을 가진다. 반면 헌법상 권리로서의 지위가 인정되지 않고 법률 차원에서 인정되는 권리도 있다. 국가에게 일정한 보호와 실현을 요구하는 디지털 권리의 경우에는 법률에 의해 인정되는 권리이거나 헌법상 권리로서의 성격을 갖더라도 법률에 의해서 비로소 구체화되는 권리인 경우가 많다. 헌법상 권리인가 법률상 권리인가에 따라 입법자의 입법형성에서 창설 여부에 대한 선택 가능성이 인정되고, 침해를 이유로 한 헌법소원심판의 인정 여부 등 법적 구제절차에서 차이가 있다.[165]

디지털 기본권으로 주장되는 것 중에는 실정헌법에서 열거된 기본권도 있고, 새롭게 도출된 기본권도 있으며, 아직 기본권성을 획득하지 못한 헌법적 가치가 있다고 주장되는 권리도 있을 수 있다. 헌법상 표현의 자유에서 파생된 익명표현의 자유가 실정헌법에 이미 열거된 기본권에 해당한다고 한다면, 새로운 독자적 기본권으로서 헌법적으로 승인된 개인정보자기결정권은 '사회적 상황의 변동'에 따라 특별한 필요성이 인정되어 기본권성을 획득한 경우에 해당한다고 할 수 있다. 다른 한편 인공지능에 대한 인간의 개입권이나 알고리즘 설명요구권 등은 그것이 헌법상 권리로서 인정될 수 있는지 그 도출 근거가 무엇인지 등에 대해서 아직 명확히 확립된 바가 없는 권리라고 할 수 있다.

기본권의 내용은 시대와 역사, 현실에 따라 그 영역경계선이 변화[166]한다고 할 때 디지털 권리 또한 헌법상 권리와 법률상 권리 간의 경계를 구분하는 것이 용이한 것은 아니다. 이 점에서도 개별 디지털 기본권의 구성요건을 분명히 하는 것은 권리의 성격과 한계, 보장의 문제를 취급하는 전제가 된다고 할 것이다.

3) 디지털 전환에 대한 기본권 형성적 법률의 제·개정

헌법상 권리가 아니라고 하더라도 디지털 권리는 법률을 통해 구체화될 수 있다. 법률을 통해 구체적으로 형성되는 디지털 권리는 실상 헌법상 권리이면서 동시에 법률상 권리이거나 헌법상 권리의 내용을 법률 단계에서 구체화한 법률상 권리인 경우가 있을 것

165) 김하열, 헌법강의 192면 참조.
166) 정종섭, 헌법학원론, 292면.

이다. 가령 개인정보보호법에 의해 인정되는 구체적인 개인정보권의 내용 형성[167]은 법률상 권리이지만, 이는 헌법상 권리인 개인정보보호의 기본권을 구체화한 것이고 이 기본권에 비추어서 평가될 수 있는 법률상 권리이다.

3. 디지털 전환에 대한 기본권 대응 체계의 정비

가. 디지털 시대 기본권의 범주화와 헌법 개정

1) 광의의 디지털 기본권과 협의의 디지털 기본권

디지털 전환에서 요구되는 특징을 별도로 취급하려고 한다면 디지털과 관련한 기본권을 범주화하여 압축된 조문에서 이를 담으려는 시도를 해 볼 수 있을 것이다. '디지털 기본권'의 명명은 설명적 범주이기는 하지만 그러한 시도의 일환이었다고 할 수 있겠다. 이는 주로 디지털의 형태로 이루어진 정보 또는 디지털 정보에 관한 기본권 및 디지털 정보의 유통과 통제에 관한 기본권(협의의 디지털 기본권)을 가리키는 것[168]으로 이해할 수 있는데, 넓게는 디지털화된 삶의 양식과 관련한 모든 기본권을 포괄할 수도 있다(광의의 디지털 기본권). 여기에는 인터넷 공간에서 집단적 의사표시를 하는 경우에 디지털 집회의 자유가 문제된다고 할 수 있을 것이고 이는 광의의 디지털 기본권으로 포섭할 수 있다. 그러나 이러한 광의의 디지털 기본권은 대부분 개별 기본권이 헌법현실의 변화에 따라 적용되는, 전통적 기본권의 내용을 가리키는 것이므로 이를 별도의 디지털 기본권으로 명명할 필요성은 크지 않고, 디지털 전환의 특수한 문제상황을 기본권 해석과 적용에서 어떻게 반영할 것인가가 주로 문제될 따름이다.

협의의 디지털 기본권으로 한정한 디지털 기본권은 그 목록이 유동적이다. 사실상 디지털 기본권과 같은 의미의 정보기본권의 범주에는 정보통신에 관한 권리로서 정보통신

167) 적극적인 정보통제권의 경우가 예가 될 수 있을 것이다. 정보통제권은 유럽연합의 디지털 권리선언과 디지털 권리장전에서 모두 발견된다.
EU 디지털 권리·원칙: 19. a 모든 사람은 EU 데이터 보호 규칙 및 관련 EU 법률에 따라 개인·비개인 데이터를 효과적으로 통제할 수 있어야 한다.
디지털 권리장전 (정보접근 통제권): 모든 국민은 디지털 환경에서 자신에 관한 정보를 열람·정정·삭제하거나 제3자에게 전송할 것을 요구하는 등 이에 대해 접근·통제할 권리를 가진다.

168) 황성기, 디지털 기본권의 의미와 내용, 헌법학연구 제24권 제3호, 2018. 9. 4면.

의 안전과 비밀 보장, 정보제공권, 알 권리, 개인정보자기결정권을 포함하는 권리[169]로 구분하거나, 정보의 자유(표현의 자유, 정보공개청구권, 정보참여권) 및 정보 프라이버시(사생활의 자유와 비밀, 개인정보자기결정권)이 있다고 한 분류 견해[170]도 있다. 디지털 기본권에 대해서는 익명표현의 자유, 인터넷접근이용권, 개인정보자기결정권, 잊혀질 권리, 디지털 정보에 대한 형사절차적 권리가 있다고 한 견해도 있다.[171]

2) 정보기본권, 디지털 기본권, 인터넷(사이버) 기본권

디지털 기본권보다 더 자주 활용되는 관련 범주의 설명개념으로 정보기본권이 있다.[172] 정보기본권은 '정보'에 관한 기본권으로서 "커뮤니케이션 매체를 통해서 유통되고 통제되는 정보에 대한 권리 내지 자유"를 가리킨다고 하며,[173] '정보기본권'의 이름으로 헌법 개정을 통해 기본권목록을 추가하려 한 시도도 있다. 정보기본권은 좀 더 넓게 "정보사회라는 새로운 생활환경에서 정보와 매체를 접근·이용하고 이를 통해 만들어진 가치를 누리며, 안전하게 믿고 이용할 수 있는 환경 등을 요구할 수 있는 헌법에서 보장하는 권리"라고 하기도 한다.[174] 정보기본권은 커뮤니케이션 매체의 속성을 가리지 않는다는 점에서 디지털 정보로 한정하는 디지털 기본권에 비해 상위개념이라고 할 수 있는데, 디지털이 관련된 영역에서의 정보기본권은 디지털 기본권과 사실상 동일한 것이다.

한편 인터넷 기본권(사이버 기본권)은 매체로서의 인터넷이라는 네트워크를 기반으로 이루어지는 디지털 기본권이다. 이 점에서는 디지털 기본권이 인터넷 기본권보다 넓은 개념이 될 수 있다.[175] 그러나 디지털 활동이 주로 인터넷을 기반으로 이루어진다는 점에서 인터넷 기본권 또한 사실상 디지털 기본권과 동일한 의미로 사용된다.

3) 헌법 개정의 문제

디지털 기본권이 기본권의 해석, 적용이나 확장을 통해 기본권적 지위가 인정되더라도

169) 김배원, 정보기본권의 독자성과 타당범위에 대한 고찰, 헌법학연구 제12권 제4호, 2006.
170) 이인호, 디지털 시대의 정보법질서와 정보기본권, 중앙대 법학논문집 26집 2호, 2002.
171) 황성기, 디지털 기본권의 의미와 내용, 헌법학연구 제24권 제3호, 2018.
172) 김상겸, 정보기본권의 체계와 보장에 관한 연구, 세계헌법연구 제7권, 2002. 12; 정필운, 정보기본권 신설 동향과 지향 - 새로운 미디어 환경을 헌법은 어떻게 수용하여야 하는가? -, 미디어와 인격권 제4권 제1호, 2018. 6.
173) 이인호, 위의 논문, 223면.
174) 정필운, 위의 논문, 5면.
175) 황성기, 위의 논문, 11면.

기본권을 명확히 실정법화할 필요가 있다고 보는 경우에는 헌법 개정을 통해 기본권 목록에 추가할 수 있을 것이다.

알 권리(정보접근권)의 경우 헌법상 기본권으로 인정되는 이상 디지털 전환과 관련하여 어떤 특별한 변화가 발생하는가는 법률과 판례를 통해서 형성해 나갈 수 있는 문제로 보이고, 디지털 전환으로 인해 이를 별도로 헌법에 추가하는 것은 의미가 크지 않다.

반면 개인정보자기결정권의 경우 그 적극적 성격으로 인해 명문화를 하는 것을 생각해 볼 수는 있을 것이다.[176] 헌법에 따라 입법례로 개인정보결정권을 별도로 입법한 예는 그러한 의의가 있는 것으로 이해된다. 특히 비교법적으로 유럽연합기본권 헌장은 제8조에서 개인정보보호권을 별도로 입법화하였고, 포르투갈 헌법 제2편("권리, 자유, 보장") 제1장("인권, 자유, 보장") 제35조는 주거 및 통신 불가침권에 대한 규정인 제34조와 가족, 결혼 및 친자관계에 대한 규정인 제36조 사이에 '정보기술 이용'에 관한 기본권(컴퓨터 기본권)을 규정하고 있다.[177]

소개한 포르투갈 헌법의 경우 디지털 기본권에 대해서 가장 적극적인 형태의 입법적 조치를 취하고 있는 예라고 할 수 있는데, 표현과 정보의 자유(Freedom of expression and information)에 대한 제37조와 언론과 매체의 자유에 대한 제38조를 두면서[178] 정보기술 이용에 관한 기본권을 별도로 인정하고 있는 것이다.

---

176) 굳이 필요하지 않다는 견해로, 김일환, 헌법 기본권편 개정의 쟁점과 대안, 공법연구 제38권 제1호, 2009. 10. 21면; 디지털 기본권(정보기본권)을 적극적으로 규정하는 것은 입법형성권에 대한 과도한 제약이 될 수도 있고 시기상조라는 견해도 있음

177) 제35조 ① 모든 국민은 법률로 정한 바에 따라 자신에 관한 모든 전산 자료에 접근할 권리, 그러한 자료를 수정 갱신할 것을 요구할 권리, 자료의 원래 사용목적에 관한 정보를 확인할 권리를 가진다.
② 개인정보의 개념을 정의하고, 개인정보의 자동 처리 및 연결, 전송 및 사용에 적용할 수 있는 자세한 조건은 법률로 정하고, 개인정보의 보호를 위한 특별 독립 행정 기관은 법률로 보장한다.
③ 사상, 정치적 신념, 정당 또는 노동조합 가입, 종교적 신조, 사생활 또는 인종 등에 관한 자료를 처리할 목적으로 정보기술을 사용해서는 안 된다. 다만 정보주체가 명시적으로 허락한 경우, 법률에 따른 권한이 있는 경우, 차별 금지를 보장하는 경우, 개인을 식별할 수 없도록 처리된 통계 자료를 처리하기 위한 경우는 예외이다.
④ 개인정보에 대한 제3자의 접근은 금한다. 단, 법률에 명시된 경우에는 예외로 허용한다.
⑤ 모든 국민에게 단 하나의 고유번호를 할당하는 행위는 금한다.
⑥ 모든 사람은 공용 정보통신망에 자유롭게 접속할 수 있는 권리를 보장받아야 한다. 다국간 데이터 이동에 적용할 기준은 법률로 정하며 개인정보에 적합한 보호 수단은 물론, 국익을 위해 정당한 방법으로 보호할 수 있는 그 밖의 자료에 대한 적절한 보호 수단도 결정한다.
⑦ 수동 파일에 수록된 개인정보는 법률로 정한 바와 같이 전항에 명시된 것과 동일한 보호를 받는다.

178) 성관정, 디지털 격차 해소를 위한 인터넷 접근권에 관한 연구: 사회적 기본권을 중심으로, 서울대학교 박사학위논문 2022. 8. 119면 또한 참조.

한편, 독일의 경우에 헌법 개정을 통한 조치로는 거주의 불가침에 관한 기본권과 관련하여 경찰 및 정보기관의 대규모 감청에 대한 규정을 추가한 사례가 있었다(제13조 제3항~제6항의 추가[179]).

우리나라의 종래 헌법 개정 논의에서는 주로 정보의 자유 형태로 헌법 개정에 반영되는 논의가 이루어졌다. 2009년 국회의장 자문 헌법연구자문위원회의 헌법개정안은 표현의 자유 조항에서 별도로 "사이버 공간의 정보유통에서도 의사표현의 자유 및 알 권리, 사적 정보의 보호는 존중되어야 하며, 국가는 정보기본권의 신장을 위해 노력하여야 한다."는 규정을 포함한 바 있고, 2014년 국회 헌법개정자문위원회 헌법 개정안은 "모든 사람은 정보문화향유권을 가진다"는 조항과 "국가는 정보격차를 해소하기 위하여 노력하여야 한다"는 조항을 추가하고자 하였다.

또 2018년 대통령 제안 헌법개정안은 제22조에서 "① 모든 국민은 알권리를 가진다. ② 모든 사람은 자신에 관한 정보를 보호받고 그 처리에 관하여 통제할 권리를 가진다. ③ 국가는 정보의 독점과 격차로 인한 폐해를 예방하고 시정하기 위하여 노력해야 한다."는 조항을 두었다.

이상의 예를 보면 정보기본권의 경우에는 실제 헌법 개정에서 그와 같은 명명이 시도된 바가 있다는 점을 알 수 있는데, 정보기본권의 구체적인 내용에 대해서는 불명확한 점이 없지 않다.

사회권적 성격을 갖는 디지털 기본권은 헌법상 인간다운 생활을 할 권리로부터 도출되는 권리, 평등권으로부터 사회권적 성격의 디지털 기본권을 도출할 여지가 있고, 헌법상 안전권이 인정된다는 전제에서 디지털 안전권 또한 안전권의 구체적 내용에 포섭할 수 있겠으나, 이러한 기본권의 구체적인 내용은 법률을 통해서 형성하는 것이 바람직하다.

나. 디지털화에서의 국가의 기본권 보장 체계

1) 기본권 존중의무 - 감시국가의 우려에 대한 경계

전통적 행정활동의 방식에서 정보기술을 활용하는 경우의 효과 또한 양면적이다. 범죄예방 및 수사를 위해 산재해 있는 디지털 데이터를 수집·저장·이용하는 활동을 함으로써

179) 1998년 3월 26일자 기본법 개정을 위한 법률 (제13조), BGBl. 1, S. 610.

사회적 안전을 강화하면서도 다른 한편으로 이른바 빅브라더(Big brother)와 디지털 감시 사회의 우려를 증폭시키는 것이다. 디지털 전환은 혁신을 통한 삶의 질 향상과 자유와 안전의 확대를 낳고 이는 기술을 활용한 범죄 추적, 안전예방과 같은 공익적 의미도 가지지만, 이는 사생활의 비밀과 자유에 대한 침해를 용이하게 하는 수단이 될 수 있다. 대표적으로 폐쇄회로 텔레비전(CCTV, Closed Circuit Television)의 확대가 이동형 영상정보처리기기(바디캠, 스마트폰, 드론, 자율주행차 등)의 활용가능성과 분석가능성 확대로 이어지면서 새로운 기본권적 문제를 낳는바, 이는 안전에 대한 욕구를 충족시켜 주면서 동시에 대규모 감시의 장치가 될수 있다. 국가적 활동의 디지털 전환 및 디지털 기술 활용은 직접적으로 디지털 전환에 따라 디지털 행정을 통해 기본권 침해가능성이 확대되는 전형적인 예에 해당한다.

사생활의 비밀과 자유는 개인의 명예, 신용, 사적 사항 등이 공개되지 않고, 평온한 사생활이 유지되며 사생활의 자율성을 간섭받지 않을 불가침적 권리를 의미하지만 디지털 심화 시대에 이를 보장하는 것은 간단한 일이 아니다. 빅데이터와 인공지능 알고리즘에 의한 사회적 감시, CCTV에 의한 대규모 군중 감시, 스마트폰을 통한 위치 추적 등 개인의 프라이버시를 침해할 수 있는 수많은 기술적 수단들이 있다.

이에 위치정보추적자료 제공요청 및 기지국수사를 할 수 있도록 한 통신비밀보호법 조항이 통신의 자유와 개인정보자기결정권을 침해한다고 본 결정[180]이나 인터넷 회선을 감청하는 이른바 패킷감청이 통신의 자유 및 사생활의 비밀과 자유를 침해한다고 한 헌법불합치 결정[181]은 디지털 사생활보호권[182]의 중요성을 인식한 데 따른 것이다.

2) 기본권 보호의무와 충족의무

디지털 기본권의 문제는 거대기업과 온라인 플랫폼과 개인 간의 관계에 개입하는 국가의 지위에서 드러나는 바와 같이 사인에 의한 기본권 침해로부터 기본권을 보호할 국가의 의무를 확인하게 한다. 오늘날 디지털 경제에서 국내외의 온라인 플랫폼의 활동으로부터 개인을 보호하기 위해 국가는 법제도를 시행하고, 절차를 마련하며, 급부를 제공

180) 헌재 2018.6. 28. 2012헌마191; 2018. 6. 28. 2012헌마538 결정.
181) 헌재 2018. 8. 30. 2016헌마263 결정
182) 디지털 권리장전 (디지털 프라이버시권) 모든 국민은 디지털 환경에서 디지털 감시, 위치 추적 등 개인의 사생활에 대한 침해와 간섭으로부터 프라이버시를 보호받을 권리를 가진다.

하여야 한다.[183]

사회권적 성격을 띄는 디지털 기본권의 경우 국가에게 충족의무를 부여한다. 개인이 기본권을 향유할 기회를 가질 수 있도록 국가는 필요한 조치를 취해야 하는 것이다. 이른바 정보접근권 및 정보향유권, 디지털 격차해소권은 헌법상 권리 또는 법률상 권리로서 국가에게 충족의무를 부여한다.

다. 사회적 형성을 통한 지속적 법제도화 필요성

앞서 본 바와 같이 유럽연합 등의 디지털 권리선언은 국내의 논의에도 일정한 영향을 미쳤는데, 정부는 지능정보사회를 대비한 종합 대책(2016. 12. 17.)을 마련한 이래[184] 최근에 이르러 디지털 전환에서의 규범적 원칙을 정립한 '디지털 공동번영 사회의 가치와 원칙에 관한 헌장: 디지털 권리장전'(2023. 9. 25. 이하 '**디지털 권리장전**')을 공개[185]하였다. 이러한 선언들의 내용은 디지털 전환에서의 기본권 전개를 전망하는 차원에서 함께 검토할 가치가 있다.

한국의 디지털 권리장전은 디지털 자유와 권리의 보장 내용으로, 안정적인 네트워크 환경을 보장받고 디지털 서비스에 차별 없이 접근하여 이용할 수 있는 권리(제6조), 디지털 환경에서 표현의 자유를 누릴 권리(제7조), 디지털 기술로 인해 차별을 받지 않고 다양성을 존중받을 권리(제8조), 디지털 개인정보에 대해 접근·통제를 할 권리(제9조), 디지털 생활양식을 강요받지 않고 대체수단을 요구할 수 있는 권리(제10조), 디지털 시대의 노동환경에서 근로·휴식할 권리(제11조)를 열거하고 있다. 이러한 내용은 대다수 헌법이 이미 보장하고 있는 기본권의 내용으로 인정할 수 있는 사항을 강조한 것으로 이해할 수 있다.

또한 디지털 권리장전은 디지털 사회를 규율하는 제도적 장치로서 정보와 기술의 독과점, 알고리즘의 불공정성 문제를 해소하여 공정한 경쟁 환경을 조성할 필요성(제12조), 디지털 자산을 보호하고 그 거래를 위한 정당한 계약이 이루어지도록 보장할 필요성(제13조), 디지털 격차를 해소하도록 디지털 리터러시에 대한 교육 기회 제공의 필요성(제14

183) 김하열, 위의 논문, 248면.
184) 관계부처 종합, 제4차 산업혁명에 대응한 『지능정보사회 중장기 종합대책』, 2016. 12. 17.
185) 디지털 권리장전의 전체 내용은 http://beingdigital.kr/front/digital_deepening.do 참조.

조), 공공 데이터를 비롯한 데이터 접근과 이용의 기회를 보장할 필요성(제15조), 디지털 심화에 따른 경제적·사회적 불평등 완화를 비롯한 사회 안전망을 강화할 필요성(제16조)을 천명하고, 디지털 기술을 윤리적으로 개발될 수 있도록 하고(제17조), 디지털로 인한 위험을 예방·관리할 수 있어야 하고 위험에 관한 정보가 공개되어야 하며(제18조), 디지털 감시, 위치추적 등을 비롯한 디지털 기술에 의해 불법적인 식별과 추적으로부터 보호되어 하고(제19조), 허위조작 및 불법·유해정보가 유통되지 않고 디지털 범죄에 대한 실효적 조치가 이루어져서(제20조), 특히 아동·청소년이 디지털 공간에서 안전하고 자유롭게 활동할 수 있어야 한다(제21조)고 하였다.

그 밖에도 디지털 권리장전은 자율과 창의가 기반을 이루는 디지털 혁신을 위해 불합리한 규제를 개선하고, 디지털 혁신을 지원하도록 하며(제22조~25조), 인류 후생을 증진하도록 지속가능한 디지털 사회를 위해 애쓰도록 하였다(제26~28조).

이상의 권리선언은 헌법 개정을 통해 디지털 기본권을 규범화하기보다 디지털화 과정에서 유념해야 할 기본권의 목록을 장전(章典) 형식(Bill of Rights, Charter)으로 원리적으로 선언하는 방식이다. 이러한 연성법은 규범력을 갖는 법원(法源)은 아니지만 디지털 권리의 기본권 및 법률상 권리로 형성해 가는 과정에서 사회적 승인과 입법화의 가이드라인이라는 의미를 가질 수 있다. 2021. 7. 발표된 스페인의 디지털 권리 헌장(Carta de Derechos Digitales), 포르투갈의 디지털 시대 포르투갈 인권 헌장(Carta Portuguesa de Direitos Humanos na Era Digital)이 예가 될 수 있다.[186] 이러한 선언은 불확실한 상황에서 섣불리 입법을 하기 이전에 상황의 변화에 대한 가이드라인을 제시하는 기능, 향후에 구체화될 입법에 대해 방향을 제시하는 기능이 주된 기능이다. 이는 디지털 전환과 같은 급격한 기술변동의 시기에 택할 수 있는 선택지라고 할 수 있다.

특히 디지털 전환의 경우 디지털 기본권과 같은 기준점이 필요하지만 이를 일국의 단위에서 관철하기 어려운 점도 선언의 형태가 활용되는 이유가 될 수 있다. 인터넷에 의한 세계화는 디지털화가 글로벌화의 다른 이름이라는 것을 상기시켜 준다. 이에 디지털화에 관한 국제사회의 선언은 일종의 헌법다원주의가 구현된 전형적 사례에 해당한다고 할 수 있다.[187]

---

186) 한국지능사회정보원(NIA), 디지털 권리 보장을 위한 선언문 및 헌장, 2023- 01.
187) Celeste, Digital Constitutionalism-The Role of Internet Bills of Rights, 62-63면 참조.

4. 디지털화된 국가서비스의 확장과 자유의 조건 보장

디지털 전환 과정은 공공 부문과 사적 부문 모두에서 진행되지만 국가는 디지털 전환과 관련하여 일종의 보장책임을 진다.[188] 그리고 한발 더 나아가 공공부문에서는 정부가 디지털 전환을 통한 사회적 급부를 제공할 직접적인 책임을 지는데, 전자적 형태의 정부 서비스 제공은 그 일환이라 할 것이다.

기존의 전자정부를 심화·발전시킨 개념인 이른바 '디지털플랫폼정부'의 추진은 공공부문 디지털 전환의 대표적 이다. 디지털플랫폼정부는 디지털 플랫폼 내에서 AI와 데이터, 클라우드컴퓨팅 등 새로운 디지털 신기술을 적용함으로써 국민들이 다양한 편익과 혜택을 누릴 수 있게 하고자 한다. 그렇다면 디지털플랫폼정부를 법제도화하는 과정에서 디지털 권리의 충실한 보장이 이루어져야 한다.

가. 디지털 포용으로서의 디지털 권리 확장

1) 디지털 선택의 자유와 접근권

디지털화에서 디지털 선택의 자유는 디지털 기술 간의 선택의 문제일 뿐만 아니라 디지털화되지 않은 삶의 양식을 선택할 수 있는 자유를 포함한다. 디지털화가 고도화될수록 아날로그화된 삶의 방식을 선택할 가능성이 불가능하거나 사실상 어려워지는 상황에 부딪힐 수 있다는 점은 디지털화가 오히려 자유를 제약할 수 있다는 것을 의미한다[189] 이는 이른바 디지털화 시대에도 아날로그 접근권(Recht auf analogen Zugang)을 어느 정도 보장할 것인가의 문제이기도 하다.[190] 이에 대해 공공영역에서 아날로그 방식의 선택가능성을 완전히 없애는 경우에는 디지털화를 허용해서는 안 된다는 입론도 소개된 바 있다.[191] 이는 이후에 인공지능기술이 발전할 경우 자신의 결정에서 자동화된 기술이 사

188) 김형섭, 보장국가와 디지털 플랫폼 정부, 한양법학 33권 제4호.
189) 성관정, 위의 박사학위논문, 27면 이하.
190) 독일의 경우 디지털 우선 정책(Digital First)에서 디지털 전용 정책(Digital Only)을 취하면서 분쟁이 발생한 바도 있다. 코로나19 관련 긴급 지원을 전자적으로만 신청할 수 있도록 한 데 대해 행정소송이 제기된 것이다. VG Wuerzburg 13. 7. 2020 – 8 E 20.815, BeckRS 2020, 16365 Rn. 7. 자세히는, Botta, 'Digital First' und 'Digital Only' in der öffentlichen Verwaltung, NVwZ 2022, 1247.
191) 조인성, 디지털 행정전환의 기본권적 허용한계와 아날로그 접근권, 일감법학 제54호, 2023. 4. 343면.

용되는 경우 그러한 서비스를 선택하지 않고서 자신의 자유와 권리를 향유할 수 있는가의 문제이기도 하다. 이는 일종의 기술에 대해 거부할 수 있는 소극적 권리로서의 문제이다. 이는 기술 변화와 관련한 일반적 행동자유권의 문제로 이해할 수도 있을 것인데, 개인이 새로운 기술 방식을 선택하거나 기술 선택의 조건을 거부하는 이유로서 자신의 기본권에 대한 제한·침해 우려가 있는 경우라면 이를 좀 더 진지하게 접근할 기회를 보장할 필요가 있다.[192]

> (디지털 권리장전) 제10조 (디지털 대체수단 요구) 모든 사람은 공공영역에서 디지털 방식을 대체하는 수단을 요구할 수 있다.

이는 구체적으로 디지털 정보에 대한 '아날로그식 접근권'의 형태로 쟁점화되기도 한다. 「지능정보화 기본법」이나 「장애인·노인·임산부 등의 편의증진 보장에 관한 법률」에서 서비스 제공자가 장애인, 노인 등이 선택에 따라 대면으로 서비스를 신청, 이용할 수 있도록 하여야 한다고 규정하는 방식을 두는 것은 입법적인 해결의 예이다.[193]

2) 디지털 포용으로서의 디지털 격차 해소권[194]

디지털 포용 정책은 앞서 언급한 디지털 격차로 인한 차별과 배제를 극복하기 위하여 디지털 기술의 혜택을 확산하기 위한 개념이다.[195] 여기서 디지털 포용(Digital Inclusion)

---

192) 이동통신기기의 사용에서 이른바 대포폰의 사용을 막기 위해 도입한 '휴대전화 가입 본인확인제'에 대한 헌법소원에서 헌법재판소는 해당 규율이 익명으로 이동통신서비스에 가입하여 자신들의 인적 사항을 밝히지 않은 채 통신하고자 하는 자들의 개인정보자기결정권 및 통신의 자유를 침해하지 않는다고 본 바 있고(헌재 2019. 9. 26. 2017헌마1209 결정), 이것이 선불폰 개통에 필요한 증서 등의 타인제공 형태로 문제된 사건에서도 이용자의 일반적 행동자유권을 침해하지 않는다고 보았다(헌재 2022. 6. 30. 2019헌가14 결정). 이에 대해서는 "통신정보 축적 및 이용자 식별의 가능성은 스스로 이동통신의 이용을 제한하는 위축효과를 발생시키기에 충분"하고 "익명통신은 이용자가 통신의 비밀과 자유를 보호하기 위하여 취할 수 있는 소수의 수단들 중 하나로서 중요한 의미를 갖는" 것이므로 "익명으로 이동통신서비스를 이용할 가능성을 완전히 배제"하는 것은 익명통신의 자유에 대한 침해라고 본 반대의견이 있었다.

193) 권건보·방동희, 고령자의 헌법적 지위와 법적 보호에 대한 고찰, 공법학연구 제24권 제1호, 2023. 2. 26면 이하.

194) 표현의 자유 관점에서 접근한 연구로 김현귀, 인터넷 접근권에 대한 연구 – 표현의 자유에 의하여 보호되는 새로운 기본권, 헌법이론과 실무(2019-A-2), 헌법재판연구원 2019. 3이 있고, 사회권적 기본권의 차원에서 접근한 연구로 성관정, 디지털 격차 해소를 위한 인터넷 접근권에 관한 연구, 서울대학교 박사학위논문 2022. 8이 있다. 후자의 연구는 인터넷 접근권의 기본권성을 인정하면서 세부적으로 인터넷 접근 환경에 관한 권리, 인터넷 접근수단에 관한 권리, 인터넷 접근역량에 관한 권리가 인정될 수 있다고 한다.

195) 원종배·이부하, 디지털 포용정책의 법제도적 내용과 발전방향, IT와 법연구 제24집, 2022. 2. 237면.

은 디지털 격차의 직접적인 대상이 되는 취약계층을 지원하는 것뿐만 아니라 전체 국민을 대상으로 디지털 기술의 접근 기회를 제공하고, 역량을 강화하는 데 목적을 두는 보편복지적 제도라고 할 수 있다. 이러한 제도의 헌법적 기반에 대해서는 정보접근권을 들고 있는데, 「지능정보화 기본법」 제46조는 국가기관등이 정보통신망을 통해 정보나 서비스를 제공할 때 장애인·고령자 등이 웹사이트와 이동통신단말장치에 설치되는 응용 소프트웨어 등 유·무선 정보통신을 쉽게 이용할 수 있도록 접근성을 보장하도록 하고 있다. 결국 정리하면 디지털 포용 정책은 소극적인 의미에서 디지털 격차를 해소하는 측면을 갖고, 적극적인 측면에서는 디지털 역량(Digital Literacy)을 강화하는 측면을 갖는다.

특히 고령층의 디지털 포용을 위해서는 디지털 접근성이 필요적으로 요구되는데, 새로운 기술 발전에 의해 고령자들은 적응의 어려움을 가질 수 있는바, 고령 친화적인 기술 환경을 제공하기 위해서는 새로운 정보통신기술에 대한 이용가능성을 좀 더 쉽게 설명하고 교육하는 기능까지도 디지털 포용을 위한 국가의 과제에 포함시킬 필요가 있을 것이다.[196] 이는 고령자의 경우 특별히 디지털 정보접근권을 광범위하게 인정할 필요가 있다는 주장[197]으로 연결되는데, 디지털 포용은 스마트 기기의 보급으로 충분하지 않고 이를 활용할 수 있는 구체적 지원책이 필요로 하기 때문이다.

다만, 사회적 취약성을 가진 고령자에 대한 법적 보호는 그것이 어떤 근거로 헌법상 정당화될 수 있는가의 문제를 낳기도 한다. 이에 대해서는, 헌법 제34조 제5항에서 "질병·노령 기타의 사유로 생활 능력이 없는 국민은 법률이 정하는 바에 의하여 국가의 보호를 받는다"는 규정이 갖는 고령자 보호에 대한 적극적 의무 부과의 의미를 강조하기도 한다.[198]

나. 자유의 조건 보장으로서 국가의 개입

사적 영역에서 전개되는 지능정보기술 발전과 그 경제적 이용 등 기본권 주체 의 자율성에 터잡은 활동과 자율적 이해관계 조정 과정을 존중하되 국가의 기본권 보장의무를 위해 일정한 경우 사적 질서에 대한 국가의 개입이 필요하다. 즉 디지털 전환에 대한 국

196) 김정수·엄주희, 디지털 시대의 소외와 포용, 그리고 공법적 대응, 법과 사회 71호, 2022. 10. 240-241면.
197) 권건보·방동희, 고령자의 헌법적 지위와 법적 보호에 대한 고찰, 공법학연구 제24권 제1호, 2023. 2.
198) 권건보·방동희, 위의 글, 6면.

가의 보장책임은 사적 부문에도 미친다. 이는 사적 영역에 대한 지원의 형태, 국가-민간의 협력 외에 필요한 경우 규제를 통해 보장책임을 이행해야 하는 경우도 있을 것이다.

V. 요약과 결론

지능정보기술의 발전에 따른 디지털 전환의 빠른 진전은 법시스템에 대한 불확실성을 증가시키고 민주적 법치국가의 헌법은 이에 대한 대응체계를 정비해야 할 도전을 받는다. 여기서 헌법의 대응체계는 디지털 전환의 리스크에 대해서 선제적으로 개입하여 사회적 편익 창출의 가능성을 사전에 완전히 차단해서는 안 될 것이고, 반대로 헌법이 보호하는 개인과 사회의 이익이 침해되도록 사회변화를 방치하여서도 안될 것인바, 디지털 전환의 사회적 편익과 리스크를 균형있게 포괄하는 헌법적 틀을 제시할 수 있어야 할 것이다.

지금까지 본 연구보고서는 디지털 전환이 초래하는 기본권적 문제상황을 소개하고 그러한 문제상황을 해소하기 위한 헌법적 요청을 어떠한 방식과 체계로 반영할 것인지를 국내외 입법과 헌법재판의 예를 중심으로 살펴보고자 하였다. 이는 디지털 전환이 갖는 특별한 문제 상황을 정확히 드러내고 헌법을 구체화하는 입법·행정·사법작용과 헌법재판 작용에서 헌법을 해석하고 실정제도화하는 데 있어 고려해야 할 점이 무엇인지를 살펴보기 위함이다.

1. 헌법해석과 헌법재판에 대한 시사점

국가작용으로 인한 기본권적 자유에 대한 해석과 적용, 제한의 한계를 심사하는 헌법재판의 측면에서 제시할 수 있는 시사점은 다음과 같은 것이 있었다.

먼저 디지털 전환의 헌법현실에서 문제되는 기본권과 그 보호범위의 설정과 관련하여 현행헌법에 따른 기본권의 적용범위와 새로운 기본권의 도출 필요성에 대해 살펴보았다.

첫째, 가령 디지털 전환으로 가상의 디지털세계가 독자적 위상을 확보할 때 '가상공간'에서 집회, 주거 등의 자유에 대해 별도의 '디지털 기본권'을 인정할 것은 아니고 기존 기본권 해석의 확장을 통해 해결하는 것이 가능한 것으로 보았다. 이것이 현행헌법의 문언해석 범위를 넘는다면 일종의 해석을 통한 헌법변천에 해당하는 경우도 있을 수 있을 것이다.

둘째, 디지털 전환의 자유 보장과 관련하여서는 우리 헌법해석에서 정착한 개인정보자

기결정권의 적용범위가 중요하다는 것을 확인할 수 있었다. 개인정보자기결정권을 인정함으로써 보호하고자 하는 헌법적 법익과 가치를 확인함으로써 그 도출근거와 적용범위를 명확히 할 필요가 있고, 그로부터 디지털전환 시대에 (독일의 IT기본권과 같이) 추가적인 기본권을 헌법으로부터 도출하거나 명문화하는 것이 필요한지에 대해 살펴보았다. 독일의 논의에서는 (지능)정보기술이 발전하면서 개인정보자기결정권이 디지털 전환에서 어떤 중추적 역할을 차지해야 하는지에 대한 시사점을 얻을 수 있었다. 독일의 논의는 개인정보자기결정권의 보장이 사생활의 핵심에 대한 보호 뿐만 아니라 개인 인격의 발현 과정에 대한 보호를 통해 궁극적으로 인간의 존엄성에 대한 충실한 보호를 도모하고자 하는 것임을 상기하게 해 준다.

셋째, IT기본권의 논의 또한 디지털 전환에서 디지털 시스템 자체에 대한 기본권적 보호의 필요성을 인식하게 하는데, 디지털 전환 과정에서 개인정보자기결정권만으로 기본권적 보장의 수요을 완전히 충족할 수 없는 영역이 존재한다고 할 때 IT기본권은 정보시스템과 기술에 대해 그 어떠한 개입의 권리 보장이 헌법적으로 요청되는 것인가의 차원에서 의미가 있다. IT기본권의 존재는 디지털 전환이 갖는 총체적 변화에 대한 대응을 위해 이 기본권이 디지털 전환에 따른 사회질서의 객관적 가치기준과 국가의 보호의무를 제시하는 의미도 가질 수 있다.

넷째, 지능정보기술과 결합한 디지털 정보(데이터) 활동이 급격히 발전하면서 종래와는 질적으로 다른 편익적·침익적 파급효과를 가져올 수 있다는 헌법현실에 대한 인식을 토대로 자유보장의 안전판으로서 개별 기본권 제한에 대한 정교한 비례성 판단이 필요하다. 앞서 비교적 자세히 언급한 독일의 위헌 결정 등에서의 세부 논증 등을 참고하여 만연히 기술발전의 안정성을 신뢰하고 남용가능성을 배제하기보다 기본권의 핵심적 가치와 기본권 제한에서 요구되는 절차와 조직에 대해 헌법적 기준을 제시할 수 있도록 비례성 판단의 논증을 전개해 나갈 필요가 있다.

2. 기본권적 가치를 반영한 법제도 형성에서의 시사점

디지털 전환에서 문제되는 기본권 보장의 맥락을 분명히 하기 위해서 기본권 목록을 추가하거나 디지털 전환의 헌법원칙을 추가하는 헌법개정을 한다면 디지털화된 헌법체계를 규범적으로 명확히 선언하는 의미가 있을 것이다. 다만, 헌법체계와 기본권 규정의 개

방성이 디지털 전환의 패러다임 전환적 성격까지 포괄할 수 있다면 현행 헌법체계에서 도출할 수 있는 디지털 시대의 가치질서와 기본권 보장으로부터 개별 법제도 형성에서의 지침을 도출하는 것도 가능할 것이다.

특히 디지털 전환을 통해 국가는 자유의 조건을 헌법적으로 형성하는 책임을 다하여야 한다. 이를 위해 현재와 같이 기술발전의 방향과 속도를 가늠할 수 없어 기본권적 위협에 대한 예측적 결정이 이루어져야 하는 경우 새로운 기술 발전의 위험에 대한 주의환기와 탄력적 대응의 필요성을 사회적으로 천명한 다음 곧바로 규제적 조치를 입법화하기보다 윤리원칙을 정립하거나 사회적 합의를 선언하는 단계 등을 거쳐 민주적 여론 수렴에 따른 입법적 규율을 해가나는 작업이 필요하다. 이에 관한 국가책임의 형성에서 다음과 같은 점에 유의할 필요가 있다.

첫째, 공적 영역에서의 디지털 전환과 관련하여 국가작용의 기본권 구속성에 유의하여야 할 것이다. 대표적으로 지능정보기술을 이용한 국가의 안보 및 질서체계 정비나 공공부문에서의 디지털 전환(전자정부 등)에서 국가작용으로 인한 기본권 침해가 발생하지 않도록 하는 것은 물론 기본권의 객관적 가치질서에 기반을 둔 제도 형성을 해 나가야 할 것이다. 공공부문의 디지털 전환에서 종래의 헌법체계에서 인정되어 온 헌법상 기본권으로서의 알 권리와 개인정보자기결정권을 토대로 기본권 주체의 정보접근권과 정보통제권을 적극적으로 형성해 나가야 할 것이다.

둘째, 디지털 전환에서 국가는 자유의 조건이 되는 기본권에 대한 보장책임을 진다. 이는 디지털 인프라의 공급이나 디지털 활동을 위한 제도 정립의 임무를 지는 것으로 표현되지만, 사회적 기본권의 차원에서 디지털 포용을 위한 디지털 격차해소권 등을 보장하는 임무도 포괄하는 것이다.

셋째, 사적 영역에서 전개되는 지능정보기술 발전과 그 경제적 이용 등 기본권 주체의 자율성에 터잡은 활동과 자율적 이해관계 조정 과정을 존중하되 국가의 기본권 보장의무를 위해 일정한 경우 사적 질서에 대한 국가의 개입이 필요하다. 이러한 과제는 경우에 따라서 일국의 주권 행사의 범위를 넘어서는 경우도 있는 어려운 과제일 수 있으나, 지능정보기술의 고도화로 인해 사적 권력이 비대하게 되는 등의 문제를 해소하기 위한 입법적 개입이 필요하다.

참 고 문 헌

1. 주요 단행본

고학수 외, 인공지능원론 – 설명가능성을 중심으로, 박영사 2021.

김하열, 헌법강의, 제6판 박영사 2024.

박희영·홍선기, 독일연방헌법재판소 판례연구 Ⅰ, 한국학술정보 2010.

성낙인, 헌법학 제23판, 법문사 2023.

이성엽 편, 데이터와 법, 박영사 2023.

이원우·김태호, 디지털 경제 전환에 대응하는 경제규제체계의 전환, 방송통신정책연구 21-17-15, 2021. 12.

이인호 외, 정보통신기술의 발전과 기본권에 관한 연구, 헌법재판연구 제25권, 헌법재판소 2014.

Di Fabio, Udo, Grundrechtsgeltung in digitalen Systemen, München 2016.

Hauser, Markus, Das IT-Grundrecht. Schnittfelder und Auswirkungen, Berlin 2015.

Heinemann, Marcus, Grundrechtlicher Schutz informationstechnischer System. Unter besonderer Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Berlin 2015.

Hoffmann, Christian et. al, Die digitale Dimension der Grundrechte: das Grundgesetz im digitalen Zeitalter, Baden-Baden 2015.

Kingreen, Thorsten/Poscher, Ralf, Grundrechte Staatsrecht Ⅱ, 38. Aufl., 2022 (정태호 역, 독일기본권론, 제33판, 2017).

Peuker, Enrico, Verfassungswandel durch Digitalisierung – Digitale Souveränität als Verfassungsrechtliches Leitbild, Tübingen 2020.

Pollicino, Oreste, Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism? Oxford 2021.

Rixen, Stephan, GG Art. 2 in: Sachs, Grundgesetz, 9. Aufl. 2021.

2. 논문

계인국, 인터넷 검색엔진과 개인정보보호-인적 관련 정보의 처리와 정보자기결정권 및 “IT-기본권”-, 법제연구 제46호, 2014. 6.

권건보, 개인정보자기결정권의 보호범위에 대한 분석-개인정보의 개념을 중심으로, 공법학연구 제18권 제3호, 2017.

권건보, 정보접근권의 실효적 보장에 관한 고찰-정보주체의 정보접근권을 중심으로-, 미국헌법연구 제29권 제2호, 2018. 8.

권건보·김일환, 지능정보시대에 대응한 개인정보자기결정권의 실효적 보장방안, 미국헌법연구 제30권 제2호, 2019. 8.

권건보/방동희, 고령자의 헌법적 지위와 법적 보호에 대한 고찰 – 고령자의 디지털 정보접근권의 보장을 중심으로, 공법학연구 제24권 제1호, 2023. 2.

김광수, 인공지능 알고리즘 규율을 위한 법제 동향 – 미국과 EU 인공지능법의 비교를 중심으로-, 행정법연구 제70호, 2023. 3.

김민호, 인터넷접근성 보장 및 국가의 역할, 성균관법학 제27권 제3호, 2015. 9.

김법연, 인공지능 통제수단으로서 주요국 규제 입법의 동향과 시사점, 유럽헌법연구 제42호, 2023. 8.

김배원, 정보기본권의 독자성과 타당범위에 대한 고찰, 헌법학연구 제12권 제4호, 2006.

김배원, 지능정보사회와 헌법 - 인공지능(AI)의 발전과 헌법적 접근 -, 공법학연구 제21권 제3호, 2020.

김영수·김일환, 독일연방헌법법원의 인구조사판결, 헌법학과 법학의 제문제, 1996.

김일환, 독일 기본법상 ‘일반적 인격권’의 성립과 발전, 법과정책 제6호, 2000.

김일환, 헌법 기본권편 개정의 쟁점과 대안, 공법연구 제38권 제1호, 2009. 10.

김일환, 지능정보사회에서 헌법의 역할과 기능, 성균관법학 제32권 제3호, 2020.

김재완, EU 일반정보보호규정(GDPR)의 알고리즘 자동화 의사결정에 대한 통제로써 설명을 요구할 권리에 대한 쟁점 분석과 전망, 민주법학 제69호, 2019. 3.

김정수/엄주희, 디지털 시대의 소외와 포용, 그리고 공법적 대응, 법과 사회 제71호, 2022. 10.

김태오, 사이버안전의 공법적 기초: 독일의 IT-기본권과 사이버안전법을 중심으로, 행정법연구 제45호, 2016. 6.

김태호, 디지털 전환기 국가-시장 관계 변화와 규제법의 과제, 경제규제와 법 제16권 제2호, 2023. 11.

김하열, 법률에 의한 기본권의 형성과 위헌심사–참정권과 청구권을 중심으로–, 고려법학 제67호, 2012. 1.

김현경, 정보주체의 권리 실효성 확보를 위한 법적 검토–개인정보에 대한 소유권 인정을 중심으로, 법학논집 제26권 제3호, 2022. 3.

김현진, 생성형 AI와 편향성, 인하대학교 IP & Data 법, 제3권 제1호, 2023. 6.

김형섭, 보장국가와 디지털 플랫폼 정부, 한양법학 33권 제4호, 2022. 11.

김희정, 알고리즘 자동의사결정으로부터 개인의 보호 – 인간의 개입권(the right to human intervention)을 중심으로, 헌법학연구 제26권 제1호, 2020. 1.

명재진, IT(정보기술) 기본권의 체계화에 관한 연구, 헌법논총 20집, 2009.

문의빈, 알고리즘 기반 추천과 플랫폼의 기본권 제한에 관한 비교법적 연구, 헌법학연구 제29권 제2호, 2023. 6.

박상돈, 정보사회의 새로운 가치를 규범화하는 헌법개정의 형태, 공법연구 제45권 제3호, 2017. 2.

박상돈, 헌법상 자동의사결정 알고리즘 설명요구권에 관한 개괄적 고찰, 헌법학연구 제23권 제3호, 2017. 9.

박원규, 인공지능, 빅데이터, 그리고 경찰 – 예측적 경찰활동에 대한 공법적 검토, 공법학연구 제24권 제1호, 2023. 2.

박희영, 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 법제 통권 제610호, 2008. 10.

박희영, 독일 연방헌법재판소의 '정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권', 인터넷법률 제45호, 2009. 1.

박희영, 최근 독일 정보기관의 정보수집권 확대와 형사정책적 시사점, 형사정책연구 제32권 제3호, 2021. 9.

백수원, 헌법상 투명성 원칙에 기반한 인공지능 규제의 방향, 성균관법학 제33권 제2호, 2021.

백수원, 알고리즘의 발달에 따른 Access권 및 알권리의 역할에 관한 시론적 고찰, 미국헌법연구 제32권 제3호, 2021. 12.

성관정, 디지털 격차 해소를 위한 인터넷 접근권에 관한 연구: 사회적 기본권을 중심으로, 서울대학교 박사학위논문 2022. 8.
소은영, 온라인 수색과 헌법상 기본권, 헌법학연구 제29권 제3호, 2023. 9.
오정하·김일환, 지능정보사회에서 알고리즘의 법·규제의 방향, 법과 정책 제27권 제3호, 2021. 12.
원종배·이부하, 디지털 포용정책의 법제도적 내용과 발전방향, IT와 법연구 제24호, 2022. 2.
이권일, 헌법상 보호되는 프라이버시 개념의 변화에 관한 소고 –독일 연방헌법재판소 판례 분석을 중심으로–, 세계헌법연구 제25권 제1호, 2019.
이권일, 디지털 데이터와 잊혀질 권리, 저스티스 통권 194-2호, 2023. 2.
이권일, 지능정보사회에서 개인정보자기결정권이 보호하고자 하는 헌법적 가치, 공법연구 제51권 제3호, 2023. 2.
이대희, 인공지능에 의한 개인정보의 자동 처리에 대한 투명성 확보에 관한 연구 - 알고리즘에 의한 자동 의사결정에 따른 '설명요구권'을 중심으로, 저스티스 200호, 2024. 2.
이동훈, 디지털사회에서의 액세스권, 헌법학연구 제11권 제2호, 2005. 6.
이부하, 디지털 사회에서 익명표현의 자유와 잊혀질 권리에 대한 법적 고찰, 홍익법학 제23권 제3호, 2022. 10.
이상학, 최근 경찰법상의 변화와 주요 쟁점–독일에서의 논의를 중심으로, 경북대학교 법학논고 제46집, 2014. 5.
이상학, 테러방지 수권규정과 기본권침해의 한계 – 독일연방수사청법의 테러방지권한에 대한 연방헌법재판소 판결 검토를 중심으로, 공법학연구 제17권 제3호, 2016. 8.
이상학, 위험방지를 위한 정보활동의 가능성과 한계–통신데이터저장제도에 관한 EU사법재판소의 판결을 중심으로, 헌법학연구 제25권 제2호, 2019. 6.
이상학, 독일 통신데이터저장법률에 관한 소고 – EU 사법재판소의 판결을 기준으로, 홍익법학 제21권 제1호, 2020. 2.
이수경, 생성형 AI의 의료적 활용과 개인정보보호, 의료법학 제24권 제4호, 2023. 12.
이인호, 디지털 시대의 정보법질서와 정보기본권, 중앙대 법학논문집 26집 2호, 2002.
이인호, 지능정보사회에서 개인정보보호의 법과 정책의 패러다임 전환, 과학기술과 법

제11권 제2호, 2020
이형석·전정환, 빅데이터를 기반으로 한 인공지능 예측력의 헌법적 쟁점에 관한 연구, 원광대학교 법학논총 제29집 제1호, 2021. 4.
이희옥, 인공지능 의사결정에서의 이익조정과 이원적 규제모델에 관한 연구, 행정법연구 제63호, 2020. 11.
이희옥, 메타버스 공간에서의 기본권 보호와 플랫폼 규제에 관한 시론적 연구, 헌법학연구 제27권 제4호, 2021. 12.
장민영, 디지털 정보접근권 실현을 위한 법적 과제, 공법학연구 22권 4호, 2021. 11.
전상현, 개인정보자기결정권의 헌법상 근거와 보호영역, 저스티스 제169호, 2018. 12.
정문식, 유럽연합 내에서 기본권보장 체계 변화, 유럽헌법연구 제36호, 2021
정애령, 독일 통신데이터저장제도의 비판적 고찰–유럽연합지침과 독일의 통신데이터저장제도 재도입 법률을 중심으로–, 공법연구 제45권 제43호, 2017. 2.
정애령, 지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호, 공법학연구 제23권 제1호, 2022. 2.
정애령, 사생활보호와 개인정보보호의 관계에 관한 연구 - 유럽연합 기본권헌장을 중심으로 -, 공법학연구 제17권 제3호, 2016. 8.
정필운, 정보기본권 신설 동향과 지향 – 새로운 미디어 환경을 헌법은 어떻게 수용하여야 하는가? 미디어와 인격권 제4권 제1호, 2018.
조소영, 지능정보사회에서 인격권의 새로운 보호체계 검토, 공법학연구 제21권 제3호, 2020. 8.
조소영, 지능정보사회에서의 기본권체계 및 보장내용의 변화 가능성 검토, 동아법학 제94호, 2022. 2.
조인성, 인터넷상 디지털 차원의 개별적 기본권에 관한 연구–독일에서의 논의를 중심으로, 홍익법학 제15권 제1호, 2014. 2.
조인성, 디지털 행정전환의 기본권적 허용한계와 아날로그 접근권, 일감법학 제54호, 2023. 4.
홍석한, 유럽연합 ‘인공지능법안’의 주요 내용과 시사점, 유럽헌법연구 제38호, 2022. 4.
황성기, 디지털 기본권의 의미와 내용, 헌법학연구 제24권 제3호, 2018.
황용석·김기태, 알고리듬 기반 자동화된 의사결정의 설명 가능성에 대한 연구, 언론정보

연구 제57권 제3호, 2020. 8.

Buermeyer, Ulf/Moini, Bijan, Gute Lücken, schlecht Lücken? Zur objektiv-rechtlichen Dimension des IT-Grundrechts, Verfassungsblog 2018. 9. 8.

Botta, Jonas, ‘Digital First’ und ‘Digital Only’ in der öffentlichen Verwaltung - Über die grundrechtlichen Zulässigkeitsgrenzen der digitalen Verwaltungstransformation und ein ‘Recht auf analogen Zugang’, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2022, 1247.

Eifert, Martin, Informationelle Selbstbestimmung im Internet, NVwZ 2008, 521.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, Neue Juristische Wochenschrift (NJW) 2010, 1035.

Kloepfer, Michael/Schärdel, Florian, Grundrechte für die Informationsgesellschaft − Datenschutz und Informationszugangsfreiheit ins Grundgesetz? Juristische Zeitung (JZ) 2009, 453.

Kühling, Jürgen, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, 681.

Hebeler, Timo/Berg, Katharina, Die Grundrechte im Lichte der Digitalisierung − Teil II/III, Juristische Arbeitsblätter (JA) 2021, 617/969.

Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009.

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042.

Luch, Anika/Schulz, Sönke, Die digitale Dimension der Grundrechte. Die Bedeutung der speziellen Grundrechte im Internet, Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR) 2013, 88.

Luch, Anika, Das neue “IT-Grundrecht”. Grundbedingung einer “Online-Handlungsfreiheit”, MMR 2011, 75.

Papier, Hans-Jürgen, Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft, NJW 2017, 3025.

Rademacher, Timo, Staatliche Überwachung, nene Technologien und die Grundrechte,

Juristische Schulung (JuS) 2020, 713.

Schliesky, Utz, Eine Verfassung für den digitalen Staat? Zeitschrift für Rechtspolitik (ZRP), 2015, 56.

Trute, Hans-Heinrich, 김태호 역, 빅데이터와 알고리즘 : 독일 관점에서의 예비적 고찰, 경제규제와 법 제8권 제1호, 2015. 5.

3. 보고서, 토론회 자료집, 인터넷 자료 등

김종현, 인공지능 법관 관련 헌법적 쟁점의 검토(2023-A-9), 헌법재판연구원 2024. 3.

김찬희, 인공지능 기반 자동화 행정행위에 관한 헌법적 고찰, 헌법이론과 실무(2023-A-3), 헌법재판연구원 2023. 9.

김태호, 바이에른 주 헌법보호법에 따른 정보기관의 정보 수집·공유 권한, 세계헌법재판 조사연구보고서 2023년 제5호, 2022. 7.

김태호, 범죄 예방을 위하여 경찰에 부여된, 자동화 시스템을 통한 데이터 처리 권한의 위헌성, 세계헌법재판 조사연구보고서 2023년 제3호, 2023. 5.

김현귀, 인터넷 접근권에 대한 연구 – 표현의 자유에 의하여 보호되는 새로운 기본권, 헌법이론과 실무(2019-A-2), 헌법재판연구원 2019. 3.

대한민국정부, 디지털 권리장전 해설서 – 23년 디지털 심화대응 실태진단 결과, 2023, 디지털공론장(beingdigital.kr).

한동훈, 유럽연합의 잊힐 권리에 관한 연구–프랑스의 경우를 중심으로–, 비교헌법재판연구(2021-B-5), 헌법재판연구원 2021. 9.

홍선기, 정보기본권 – 독일 및 EU를 중심으로, 한국법제연구원 연구보고서 2018.

한국지능사회정보원(NIA), 디지털 권리 보장을 위한 선언문 및 헌장–EU·스페인·포르투갈 사례, 2023-01, 2023.

Baum/Kurz/Schantz, Das vergessene Grundrecht, Frankfurter Allgemeine Zeitung, 2013. 2. 26.

European Declaration on Digital Rights and Principles, 2030 Digital Compass.

디지털 전환의
기본권적 문제상황과 대응체계

2024年 3月 19日 印刷
2024年 3月 26日 發行

발 행 : 헌 법 재 판 소
헌법재판연구원

인 쇄 : 성문인쇄사(02·2272·7553)